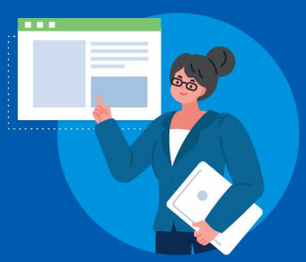
2022년

사이버보안 대연합(2차)

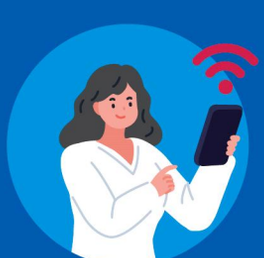


CONTENTS

탐지공유 분과

대응역량 분과

정책제도 분과



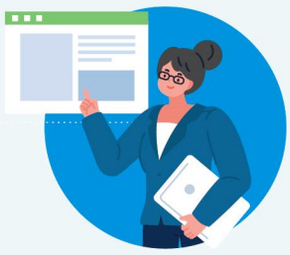
KISA 한국인터넷진흥원 kisia 한국정보보호산업협회

사이버보안 대연합

2022년 11월 9일 인쇄
2022년 11월 9일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원



2022년
사이버보안 대연합

탐지공유 분과

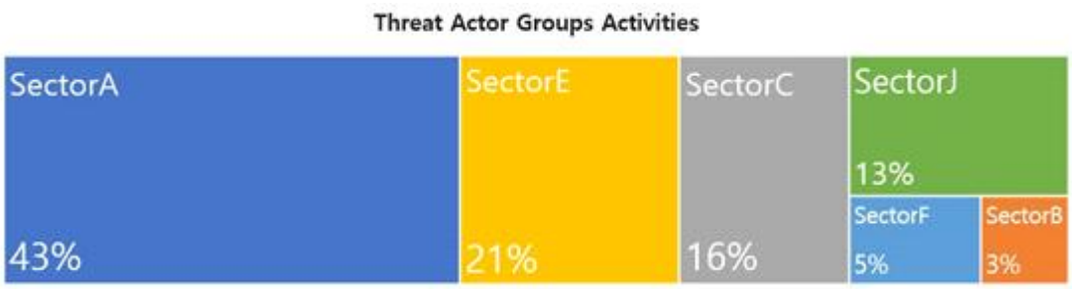
1. 글로벌 해킹그룹 동향보고서 [장영준 수석, NSHC]
2. IATinfect.exe, Shadow Force 그룹의 비밀 무기 [차민석 수석, 안랩]

글로벌 해킹그룹 동향보고서

장영준 수석, NSHC, cyj@nshc.net

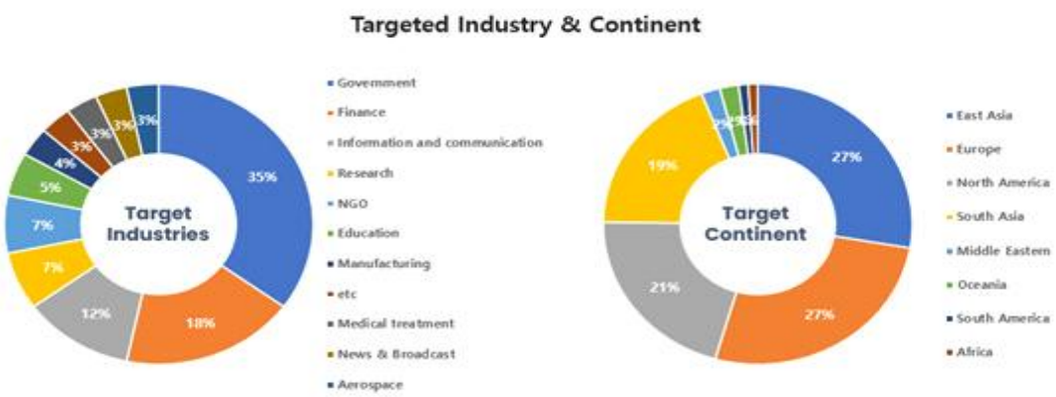
1. 개요

2022년 7월 21일에서 2022년 8월 20일까지 수집된 데이터와 정보를 바탕으로 NSHC ThreatRecon팀에서 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다.
이번 8월에는 총 20개의 해킹 그룹들이 확인되었으며, SectorA 그룹이 43%로 가장 많았으며, SectorE와 SectorC 그룹들의 활동이 그 뒤를 이었다.



[그림 1] 2022년 8월에 확인된 해킹 그룹별 활동 통계

이번 8월에 발견된 해킹 그룹들의 해킹 활동은 정부부처와 금융 산업군에 종사하는 관계자 또는 시스템을 대상으로 가장 많은 공격을 수행했으며, 지역별로는 동아시아(East Asia)와 유럽(Europe)에 위치한 국가들을 대상으로 한 해킹 활동이 가장 많은 것으로 확인된다.



[그림 2] 2022년 8월 공격 대상이 된 산업 분야와 국가 통계

1) SectorA 그룹 활동 특징

SectorA 그룹들 중 이번 8월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA01, SectorA02, SectorA05, SectorA06, SectorA07 그룹이다.

SectorA01 그룹은 중국, 영국, 브라질, 터키 미국, 인도, 싱가포르에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 금융, IT, 항공우주, 제조 등의 산업군에 종사하고 있는 관계자들을 대상으로 특정 암호화폐 거래소의 엔지니어 채용 문서로 위장한 악성코드를 배포했다.

SectorA02 그룹의 활동은 한국에서 해킹 활동이 발견되었다. 해당 그룹은 '업무연락', '거래내역' 등의 문서 파일로 위장한 악성코드를 배포하였으며, 한국의 인력 파견 서비스 기업의 웹 서버를 장악해 C2 서버로 악용하고 있다.

SectorA05 그룹은 한국, 미국에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 NFT(Non-Fungible Token) 보상 토큰 공지 내용으로 위장한 스피어 피싱(Spear Phishing) 이메일을 발송했다.

SectorA06 그룹의 활동은 홍콩, 영국, 미국, 인도, 중국, 이탈리아, 러시아에서 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 금융 산업에 종사하고 있는 관계자들을 대상으로 윈도우 바로가기(LNK) 파일 형식의 악성코드를 배포했다. 해당 악성코드는 공격 대상이 관심을 가질 만한 채용, 급여 협상, 수익 분배 등의 파일명으로 위장하고 있다.

SectorA07 그룹은 러시아, 한국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 템플릿 인젝션(Template Injection) 기법을 사용하는 MS 워드(Word) 형식의 악성코드를 배포했다. 해당 워드 형식의 악성코드는 한국의 특정 대학교 한국어교육원에서 작성한 문서로 한국의 특정 보안솔루션으로 검증한 안전한 문서로 위장하고 있다.

현재까지 계속 지속되는 SectorA 해킹 그룹들은 한국과 관련된 정치, 외교 활동 등 정부 활동과 관련된 고급 정보를 수집하기 위한 목적을 가지며 전 세계를 대상으로 한 금전적인 재화의 확보를 위한 해킹 활동을 병행하고 있다. 이들의 해킹 목적은 장기간에 걸쳐 지속되고 있으며, 이러한 전략적 해킹 목적으로 당분간 변화 없이 지속적으로 진행될 것으로 판단된다.

2) SectorB 그룹 활동 특징

SectorB 그룹들 중 이번 8월 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB03 그룹이다.

SectorB03 그룹은 체코, 필리핀, 태국, 베트남, 영국, 중국, 벨기에, 헝가리, 싱가포르에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 특정 비디오 채팅 앱(Video Chatting App) 서버를 장악하여, 사용자가 정상적인 경로에서 다운로드 받은 설치 프로그램에서 다른 악성코드를 추가로 받아오도록 변조하였다.

현재까지 지속되는 SectorB 해킹 그룹들의 해킹 활동 목적은 전 세계를 대상으로 각국 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 것으로 분석된다.

3) SectorC 그룹 활동 특징

SectorC 그룹들 중 이번 8월 총 2개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorC08, SectorC14 그룹이다.

SectorC08 그룹은 우크라이나, 미국, 러시아, 필리핀, 독일, 스웨덴, 스페인, 인도, 프랑스에서 이들의 활동이 발견되었다. 우크라이나 관련 문서로 위장한 MS 워드 파일 형식의 악성코드를 사용했으며, 최종적으로 원격 제어 도구인 울트라 VNC(UltraVNC)를 사용했다.

SectorC14 그룹은 미국, 영국에서 이들의 활동이 발견되었다. 해당 그룹은 국방, 비정부 기구(NGO), 정부간 국제기구(IGO) 등을 대상으로 소셜 네트워크(Social Network) 서비스를 사용하여 공격 대상과 신뢰를 구축하는 사회공학(Social Engineering) 기법을 사용했다. 그리고, 공격 대상을 피싱 사이트 접속을 유도하여 공격 대상의 메일 계정 로그인 정보를 탈취하였다. 최종적으로 오픈 소스 원격 제어 도구를 통해 시스템 원격제어를 시도했다.

현재까지 지속되는 SectorC 해킹 그룹들의 해킹 활동은 인접한 국가를 포함한 전 세계를 대상으로 각 국가들의 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

4) SectorE 그룹 활동 특징

SectorE 그룹들 중 이번 8월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE02, SectorE03, SectorE04, SectorE05그룹이다.

SectorE01 그룹은 파키스탄, 루마니아, 인도, 중국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 템플릿 인젝션 기법을 사용하는 파키스탄 정부 및 국방부 문서로 위장한 MS 워드 파일 형식의 악성코드를 배포했다.

SectorE02 그룹은 우크라이나, 파키스탄, 싱가포르, 네덜란드, 방글라데시, 인도, 오스트리아, 러시아에서 이들의 해킹활동이 발견되었다. 해당 그룹은 이번 활동에서 회의록 양식, 부품 재고 부족, 편지 등의 제목으로 위장한 MS 워드 파일과 RTF(Rich Text Format) 등의 문서형 악성코드를 배포했다.

SectorE03 그룹은 이번 활동에서 PE(Portable Executable) 형식의 악성코드를 공격 대상 시스템에 설치하고 시스템 제어권을 탈취하는 전술을 사용하고 있다.

SectorE04 그룹은 필리핀에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 2022년 회의록 PDF 파일로 위장한 바로가기(LNK) 형식의 악성코드를 압축한 파일을 유포했다.

SectorE05 그룹은 파키스탄, 미국, 인도, 영국, 뉴질랜드에서 이들의 활동이 발견되었다. 해당 그룹은 이번 활동에서 정교하게 만들어진 가짜 웹 사이트에서 공격 대상이 직접 안드로이드 악성코드를 다운로드 하도록 유도하였다.

현재까지 지속되는 SectorE 해킹 그룹들의 해킹 활동 목적은 인접한 파키스탄 정부와 관련된 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다. 그러나 최근에는 중국을 포함한 극동 아시아와 다른 지역으로 확대되고 있는 점으로 미루어, 정치, 외교 및 기술 관련 고급 정보들을 획득하기 위한 활동의 비중도 커지고 있는 것으로 분석된다.

5) SectorF 그룹 활동 특징

SectorF 그룹들 중 이번 8월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorF01그룹이다.

SectorF01 그룹은 중국, 홍콩, 터키, 베트남, 이탈리아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 이번 활동에서 규제 및 법률 위반 관련 자료 및 마케팅 광고 등의 제목으로 위장한 MS 워드 파일 형식의 악성코드를 배포했다.

현재까지 SectorF 해킹 그룹은 이들을 지원하는 정부와 인접한 국가들의 정치, 외교 및 군사 활동과 같은 고급 정보를 수집하기 위한 목적과, 자국의 경제 발전을 위한 첨단 기술 관련 고급 정보 탈취를 위한 목적을 갖는 것으로 분석된다.

6) 사이버 범죄 그룹 활동 특징

온라인 가상 공간에서 활동하는 사이버 범죄 그룹은 이번 8월에는 총 6개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ01, SectorJ04, SectorJ14, SectorJ20, SectorJ26, SectorJ31 그룹이다.

이들은 다른 정부 지원 해킹 그룹들과 다르게 현실 세계에서 금전적인 이윤을 확보할 수 있는 재화적 가치가 있는 온라인 정보들을 탈취하거나, 직접적으로 특정 기업 및 조직들을 해킹 한 후 내부 네트워크에 랜섬웨어(Ransomware)를 유포하거나, 중요 산업 기밀을 탈취한 후 이를 빌미로 금전적 대가를 요구하는 협박 활동 등을 수행한다.

SectorJ01 그룹의 활동은 미국에서 발견되었다. 해당 그룹은 송장 관련 파일로 위장한 XLL(마이크로소프트 엑셀의 추가 기능 파일) 형식의 악성코드를 사용했으며, 시스템 기본 정보, 프로세스 목록 등 다양한 정보를 수집하여 C2 서버에 전송한다.

SectorJ04 그룹의 활동은 오스트리아, 독일에서 발견되었다. 해당 그룹은 의료 및 건강 관련 회사를 대상으로 피싱 메일을 전송했으며, 이력서로 위장한 바로가기(LNK) 파일을 압축하여 IMG 형식의 압축 파일을 첨부했다.

SectorJ14 그룹의 활동은 프랑스, 미국에서 발견되었다. 해당 그룹은 여러 국가들을 대상으로 안드로이드 스마트폰의 정보를 탈취하기 위한 목적으로, 크롬(Chrome) 웹 브라우저로 위장한 안드로이드 악성코드를 사용했다.

SectorJ20 그룹의 활동은 말레이시아, 미국, 중국, 네덜란드, 리투아니아, 불가리아, 나이지리아에서 발견되었다. 해당 그룹은 스피어 피싱 메일에 포함한 원드라이브(OneDrive) 링크를 전달하여, 바로가기(LNK) 파일 형식의 악성코드가 압축된 ISO파일을 다운로드 받도록 유도했다.

SectorJ26 그룹의 활동은 미국, 독일, 프랑스에서 발견되었다. 해당 그룹은 법률 회사 및 항공 업체를 대상으로 비용 청구서, 이력서 또는 법률 관련 문서로 위장한 MS 워드 파일 형식의 악성코드를 첨부한 스피어 피싱 메일을 전달했다.

SectorJ31 그룹의 활동은 독일, 헝가리, 네덜란드에서 발견되었다. 해당 그룹은 공격 대상 조직의 개인 구글 계정 자격 증명을 획득한 후, 외부에 노출된 VPN 서버의 인증을 통해 공격 대상 조직의 시스템 내부에 접근했다.

IATinfect.exe, Shadow Force 그룹의 비밀 무기

Shadow Force 그룹의 특징과 습관

차민석 수석, 안랩, minseok.cha@ahnlab.com

사이버 공격은 완전 자동화가 아닌 상당 부분 사람에 의해 이뤄진다. 사람의 특성상 공격자도 익숙한 공격 방식을 선호하고, 사용하는 악성코드나 도구도 유사한 경우가 많다. 어떤 공격자는 10년 넘게 동일한 방법과 도구를 사용하기도 한다. 보안 연구가들은 위협그룹(Threat Actor)을 구분할 때 위협 해위자의 독특한 습관을 이용하기도 한다.

2013년부터 한국에서 활동하고 있는 Shadow Force 그룹도 독특한 특징이 있으며 이런 특징을 이용해 내부 침해 여부를 확인할 수 있다.

1. Shadow Force 그룹

1) 소개

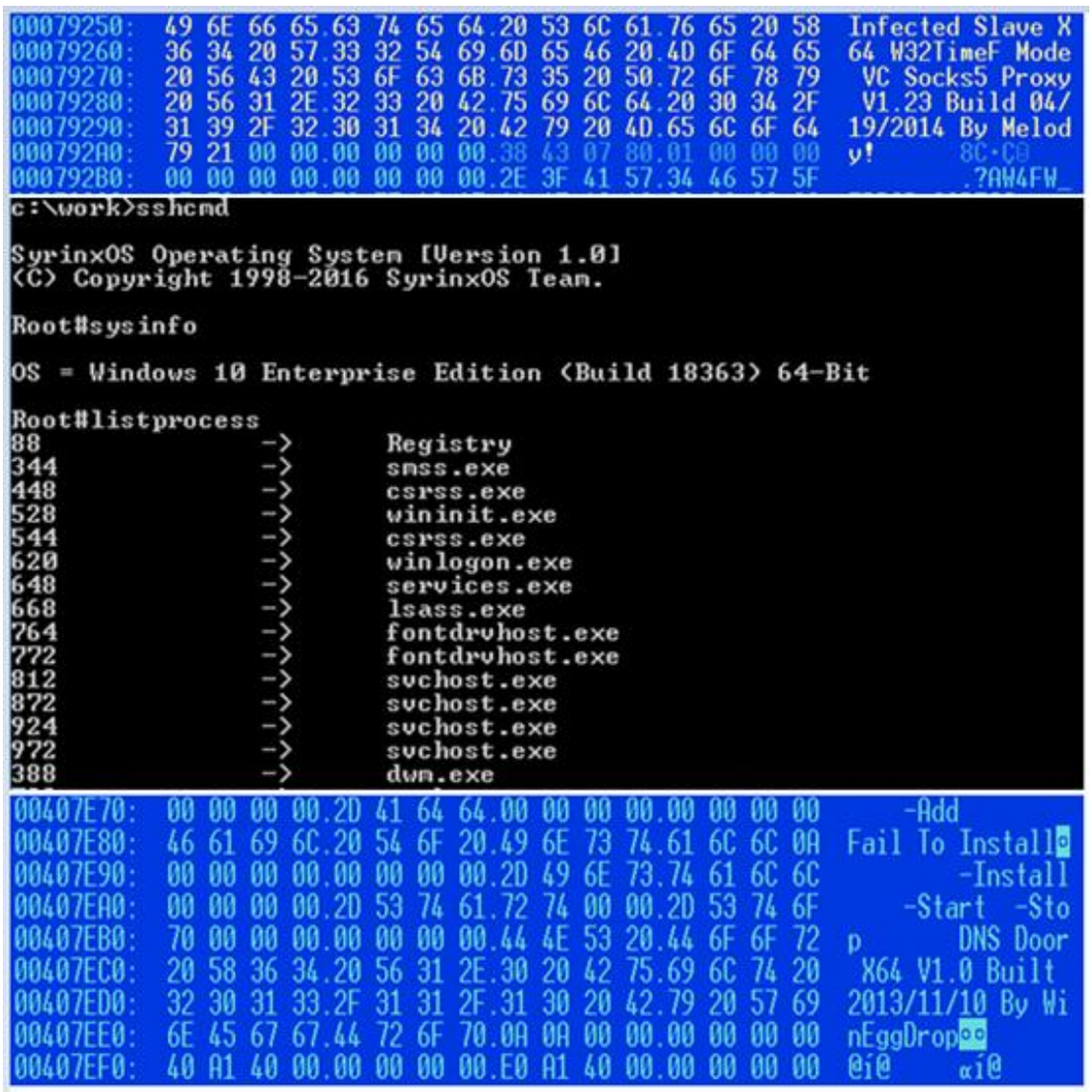
Shadow Force (쉐도우포스) 그룹은 2013년부터 활동하고 있는 위협그룹으로 대한민국 기업과 기관을 목표로 하고 있다. 2015년 9월 트렌드마이크로에서 최초 분석 보고서를 공개[1]했으며 한국의 미디어 관련 회사를 공격했다고 한다. 2020년 3월 안랩은 'Operation Shadow Force' 분석 보고서를 공개[2]한다. 최초 공개할 때는 어떤 위협그룹의 소행인지 확인되지 않아 위협 그룹이 아닌 하나의 캠페인으로 공개했으며 분석보고서가 공개된 후 2년이 넘게 한국 이외에서 감염보고나 추가 관련 보고서가 공개되지 않고 있어 현재는 한국에서 활동하는 위협 그룹으로 판단하고 있다. 2022년 7월 KRCert는 'TTPs#7 SMB Admin Share를 활용한 내부망 이동 전략 분석'[3]을 통해 Shadow Force의 추가 침해 사고 분석 내용을 공개했다.

Shadow Force 그룹은 한국에서 활동 중인 다른 유명 그룹에 비해 잘 알려지지 않았지만 10년 동안 꾸준히 활동하고있다. 이들은 중국어 도구를 주로 사용하며 악성코드에 멜로디(Melody), 시링크스(Syrinx), 윈에그드롭(WinEggDrop)와 같은 제작자 이름을 남겨 두기도 한다.

악성코드 내에 자신들의 닉네임을 남겨두는 등 국가 후원을 받고 있다고 추정되는 위협 그룹과는 다른 특징을 가지고 있어 사이버범죄 조직에 가깝지 않을까 추정되지만 한국만 공격 중인지 그렇다면 왜 한국만 공격하는지는 확인되지 않았다.

1) http://documents.trendmicro.com/assets/pdf/shadow-force-technical-brief.pdf
2) https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=29129
3) https://boho.or.kr/data/reportView.do?bulletin_writing_sequence=66830

[그림 1] 악성코드에서 발견된 제작자 별명



2) 공격 방법

피해 시스템은 보통 윈도우 서버이며 공격자가 어떤 방법으로 시스템에 침해했는지는 알려지지 않았다. KRCert에 따르면 SMB/Admin Share를 통해 내부 전파 (Lateral Movement)가 이뤄진다고 한다.

Htran (보통 aio.exe 혹은 aiom.exe)은 해킹을 위한 파일 업로드와 다운로드, 파일 실행, 계정 생성 및 삭제, 로그 삭제, 프로세스 숨기기, 서비스 등록, 로그 오프, 포트 매핑, 시스템 종료와 재부팅 등 다양한 기능을 제공하는 도구이다. SQL 관련 파일인 sqlservr.exe 파일에서 aio.exe 파일을 다운로드 한 기록이 있어 공격자는 SQL 서버를 장악 후에 aio.exe 파일을 다운로드 했다고 생각된다.

Htran을 실행화면은 다음과 같다.

[그림 2] aio.exe 주요 기능

aio.exe를 통해 다운로드 되는 파일 중 iatinfect.exe 혹은 iat.exe 파일 이름의 Pemodifier는 윈도우 실행 파일을 변조한다. 보통 사용자가 신뢰하거나 자주 실행하는 파일을 변조하며 사용자가 변조된 파일을 실행할 때 Shadowforce 같은 악성코드가 함께 로딩된다. 마지막으로 화면 캡쳐나 키로깅 기능을 가진 프로그램을 통해 사용자를 감시한다.

[그림 3] Shadow Force 그룹의 악성코드와 도구

3) 주요 공격 대상 및 사례

다음은 Shadow Force 그룹의 침해가 확인된 기업이다.

[표 1] Shadow Force 그룹 침해가 확인된 기업

일 시	공격 대상	내 용
2014년 9월	IT 운영관리	Htran, Pemodifier, Wgdrop 등을 이용한 공격
2015년 1월	의료	VAN 관리 프로그램 패치 해 Wgdrop B형 실행
2015년 5월	언론사	Shadowforce 변형 접수
2015년 7월	운송	Shadowforce, Pemodifier 발견
2015년 8월	외식	Wgdrop A형과 시스템 관리 프로그램 변조해 Wgdrop B형 실행
2019년 3월	정치기구	ShadowForce 변형 신고

하지만, 실제 피해를 입은 업체가 더 존재한다. 안랩에서도 신고를 통해 감염이 확인된 업체는 몇 곳 없지만 피해 업체가 확인되지 않은 감염 사례가 30 곳 이상 존재한다.

이들은 시스템 사용에 지장을 주지 않아 감염 사실을 모르는 경우도 많다. KRCert 보고서에도 피해 업체가 수년 동안 공격자에게 장악 당했지만 연락 받기 전까지 감염 사실을 몰랐다고 한다.

2. iatinfect.exe 혹은 iat.exe

공격자는 aio.exe 파일을 이용해 여러 도구를 다운로드하고 사용하는데 iatinfect.exe 혹은 iat.exe 파일 이름의 PE 파일 변조 프로그램 Pemodifier를 즐겨 사용한다.

Pemodifier로 지정한 EXE 파일을 변조해 특정 DLL 파일을 로드하는 도구이다. 2014년 9월부터 2022년 2월까지 총 34개 변형이 확인되었으며 파일 이름은 30개 이상에서 iatinfect.exe를 사용했다. 파일 길이는 31,744 바이트에서 1,036,288 바이트 정도되며 2020년 이후 발견된 변형은 100 킬로바이트 정도의 파일 길이를 가진다.

제작자 이름은 다른 악성코드도 제작한 WinEggDrop이지만 파일 내부에는 다른 제작자의 별명인 Syrinx도 포함되어 있다. 전체 도구는 WinEggDrop이 제작하고 PE 파일 감염 부분은 Syrinx가 제작했을 가능성이 높다.

현재까지 iatinfect.exe나 iat.exe 파일이 발견된 경로는 다음과 같다.
iatinfect.exe 파일은 32비트 버전과 64비트 버전이 존재하며 초기 버전은 프로그램 버전을 출력한다.

[표 2] iatinfect.exe, iat.exe 파일 발견 경로

No.	경 로
1	C:\Intel
2	C:\PerfLogs
3	C:\Windows\System32
4	C:\Windows\logs
5	C:\Users\[사용자계정]\desktop

[그림 4] iatinfect.exe 실행 화면

```
c:\work>iatinfect
PE File Infector V1.0 Built 06/25/2014 By WinEggDrop

c:\work>iatinfect
PE File Infector X64 V1.0 Built 2014/09/24 By WinEggDrop

c:\work>iatinfect
PE File Infector V1.0 Built 2014/10/31 By WinEggDrop

c:\work>iatinfect
PE File Infector V1.0 Built 2014/11/29 By WinEggDrop

c:\work>iatinfect
PE File Infector X64 V1.0 Built 2014/11/29 By WinEggDrop

c:\work>iatinfect
PE File Infector X64 V1.0 Built 2015/09/03 By WinEggDrop
```

지금까지 발견된 변형의 프로그램 정보는 다음과 같다.

[표 3] iatinfect.exe, iat.exe 파일 발견 경로

No.	버전 정보
1	PE File Infector V1.0 Built 06/25/2014 By WinEggDrop
2	PE File Infector V1.0 Built 06/26/2014 By WinEggDrop
3	PE File Infector V1.0 Built 06/27/2014 By WinEggDrop
4	PE File Infector V1.0 Built 09/18/2014 By WinEggDrop
5	PE File Infector V1.0 Built 2014/10/31 By WinEggDrop
6	PE File Infector V1.0 Built 2014/11/29 By WinEggDrop
7	PE File Infector V1.0 Built 2015/06/13 By WinEggDrop
8	PE File Infector V1.0 Built 2015/09/03 By WinEggDrop
9	PE File Infector X64 V1.0 Built 03/22/2020 By WinEggDrop
10	PE File Infector X64 V1.0 Built 09/18/2014 By WinEggDrop
11	PE File Infector X64 V1.0 Built 2014/09/24 By WinEggDrop
12	PE File Infector X64 V1.0 Built 2014/11/10 By WinEggDrop
13	PE File Infector X64 V1.0 Built 2014/11/29 By WinEggDrop
14	PE File Infector X64 V1.0 Built 2015/06/13 By WinEggDrop
15	PE File Infector X64 V1.0 Built 2015/09/03 By WinEggDrop

하지만, 2020년 4월 이후 발견된 변형의 파일 이름은 iatinfect.exe로 동일하나 프로그램 정보를 표시하지 않는다.

프로그램 정보를 출력하지 않는 변형도 주요 문자열을 암호화하고 있지 않아 'infect IAT OK' 등의 의심스러운 문자열을 파일에서 찾을 수 있다.

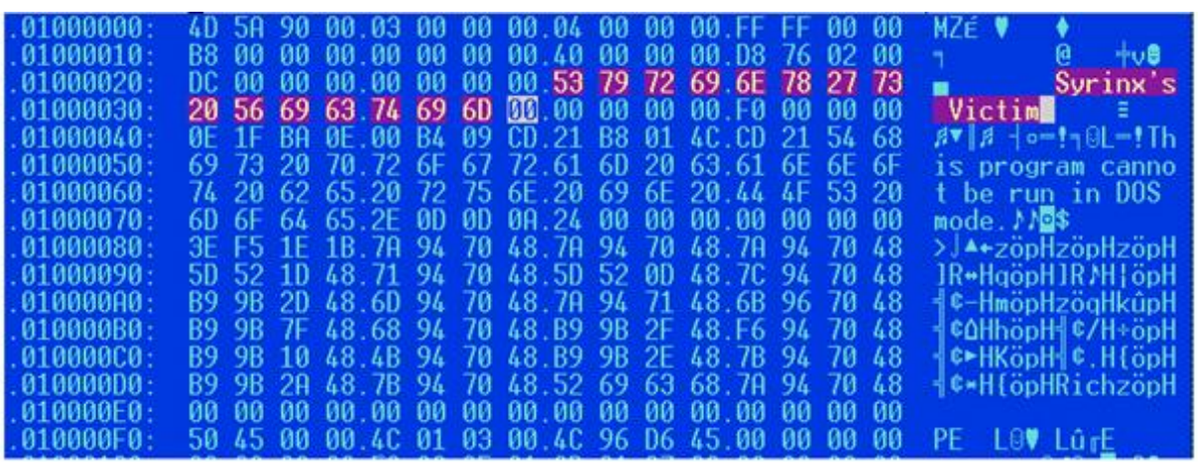
[그림 5] iatinfect.exe의 특징적 문자열

공격자는 사용자가 신뢰하는 프로그램을 주로 패치하며 현재까지 확인된 파일이름은 armsvc.exe, cissesrv.exe, cpqrcmc.exe, EmSvr_Mail.exe, ImageSAFERSvc.exe, mstsc.exe, NCleanService.exe, npesvc.exe, sqlservr.exe, Sqlwrite.exe, srvany.exe, UBiz5.exe 등이다.

보통 악성코드가 윈도우가 시작될 때 자동 실행되지만 이 그룹은 사용자가 특정 프로그램을 실행할 때 악성코드가 함께 로드되어 상대적으로 발견하기 어렵다.

iatinfect.exe로 패치 된 파일은 파일 헤더 내에 'Syrinx's Victim' 문자열이 추가된다.

[그림 6] 변조된 파일의 특징적 문자열



시스템에서 iatinfect.exe나 iat.exe 파일이 발견된다면 이 그룹의 공격을 받았을 가능성이 높다.

3. 결론

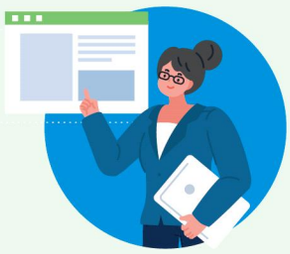
위협 그룹은 주기적으로 악성코드나 도구를 변경하기도 하지만 몇 년 동안 동일한 도구를 사용하는 경우도 있다. Shadow Force 그룹은 2013년부터 활동하며 10년 가까이 동일한 파일 이름의 도구를 사용하고 있다. 잘 알려지지 않았지만 Shadow Force 그룹은 한국에서 꾸준히 활동하고 있으므로 공격자의 변경하지 않는 이런 습관을 이용하면 침해 사실을 좀 더 빠르게 파악할 수 있다. 보안 담당자가 침해 여부를 빠르게 발견할 수 있게 다양한 위협 그룹의 특징이 공유되어야 한다.

4. 참고 자료

[1] Shadow Force Uses DLL Hijacking, Targets South Korean Company
(https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company)
(http://documents.trendmicro.com/assets/pdf/shadow-force-technical-brief.pdf)

[2] 정상 인증서에 숨은 섀도 포스, 7년간의 행적 드러나
(https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=29129)

[3] TTPs#7 SMB Admin Share를 활용한 내부망 이동 전략 분석
(https://boho.or.kr/data/reportView.do?bulletin_writing_sequence=66830)



2022년
사이버보안 대연합

대응역량 분과

1. Yanluowang Ransomware Gang 분석자료 [최재우 이사, 에스케어]
2. 2022년 주요 랜섬웨어 및 대응 방안 [김건우 실장, 안랩]

Yanluowang Ransomware Gang 분석자료

최재우 이사, 에스케어, jw.choi@escare.com

1. Executive Summary

- Yanluowang Ransomware Gang은 2021년 8월 Symantec에 의하여 최초 언급되었으며, 미국 기업을 표적으로 하여 활동을 하는 것으로 조사됨
- 2021년에는 랜섬웨어 공격을 수행한 후 피해자가 복호화 키를 위한 가상화폐를 지불하지 않으면 DDOS 공격을 수행함
- 2022년에는 랜섬웨어 공격을 수행한 후 피해자가 복호화 키를 위한 가상화폐를 지불하지 않으면 고객의 데이터를 공개하는 암호화 및 정보유출 위협행위를 수행함
- 금융 기업이 주요 표적이지만 IT 서비스, 제조, 컨설팅 및 엔지니어링 회사도 공격함
- Lapsus$의 하위 조직으로 분석되며, 2022년 8월에는 Cisco를 공격하였다고 발표함
- 2022년 5월 이들은 Cisco를 침해하였다고 주장하였지만, Cisco는 내부정보 유출에 대하여 사실 무근이라고 발표함
- 2022년 8월 Cisco 대변인은 랜섬웨어 공격자들이 Cisco의 자료를 다크 웹에 공개했다고 인정했으며 Cisco는 밝혀낸 공격 방식을 외부에 공개함
- Cisco는 최초 공격이 실제로 UNC2447 사이버 조직 및 Lapsus$ 공격자 그룹을 비롯한 다른 그룹과 연결된 초기 액세스 브로커에 의해 시작되었다고 발표함
- 2022년 6월 이들은 미국의 다국적 소매 기업 Walmart를 랜섬웨어 공격의 피해자 목록에 추가했다고 주장함
- 이들은 Walmart의 40,000~50,000대의 컴퓨터를 암호화하고 침해 기간 동안 해당 회사의 데이터를 유출했다고 주장함

2. 사례 학습

- 최근 해킹그룹은 FireEye, Microsoft, Cisco와 같은 보안 기업을 무력화하는 공격을 수행함
- 기업이 이런 공격을 막으려면 최신 공격을 방어할 수 있는 고도화된 보안 기술에 집중해야 함
- 밝혀진 공격을 빠르게 대응하기 위한 인텔리전스 도입, 알려진 취약점에 대한 빠른 공격 표면관리, 자동화 조치 체계의 도입이 필요함
- 사이버 하이진이 고려된 취약점 점검 및 대응, 공격표면 자동화 점검 및 조치, 동종 업계 공격 동향 수집 및 사전 방어체계 구축, 유명 공격그룹에 대한 TTP 대응 전략 수립을 통해 위협이 내부로 향하기 전에 고도화된 방어체계 수립이 필요함

3. Cisco 침해 개요

2021년 10월에 처음 발견된 Yanluowang 랜섬웨어는 미국에 기반을 둔 기업에 대한 표적 공격에 자주 사용되는 랜섬웨어 유형입니다. 그 이름은 지옥의 10대 천왕 중 하나인 중국의 신 Yanluo Wang을 지칭합니다.

Yanluowang TOR 유출 페이지에 따르면 이 랜섬웨어의 배후 공격자들은 2021년 10월부터 6개 이상의 산업 분야에서 기업을 손상시켰습니다. 또한 연구원들은 Yanluowang 운영자가 이전에 Thieflock 랜섬웨어에 연결된 TTP(전술, 기술 및 절차)를 사용하는 것을 관찰했습니다.

과거 공격에서 이런 공격자는 정찰 및 데이터 수집 활동을 위해 AdFind(Active Directory에서 정보를 수집하는 무료 명령줄 쿼리 도구), netscan.exe 및 SoftPerfect Network Scanner와 같은 오픈 소스 도구를 활용했습니다.

2022년 8월 10일 Yanluowang 랜섬웨어 범죄 조직은 테크놀로지 대기업 Cisco에서 유출한 데이터를 아래 이미지와 같이 게시했습니다. Cisco는 2022년 5월 말에 이 침해 사실을 공개했습니다. Cisco는 “Cisco 제품 또는 서비스, 민감한 고객 데이터나 직원 정보, 지적 재산이나 공급망 운영에는 영향이 없다”고 주장합니다.

[그림 1] Yanluowang Ransomware

Cisco confirms compromise as ransomware group publishes a partial list of files it claims to have exfiltrated. Cisco also confirmed that only pre-ransomware activity was observed and that actual ransomware deployment was not identified.

그러나 Cisco 알림은 랜섬웨어의 사전 활동에 관해서만 설명했을 뿐 회사 네트워크의 랜섬웨어 배포를 발견하지 못했습니다. Cisco의 기업 환경에서 식별된 이런 TTP는 대규모 랜섬웨어 배포를 위한 공격자의 일반적인 준비 활동이었습니다.

이 Cisco 사건에는 공격자가 브라우저 자격 증명 동기화를 통해 직원의 개인 Google 계정을 손상시키고 회사 자격 증명을 손상해 Cisco 기업 리소스에 액세스한 증거들이 있습니다.

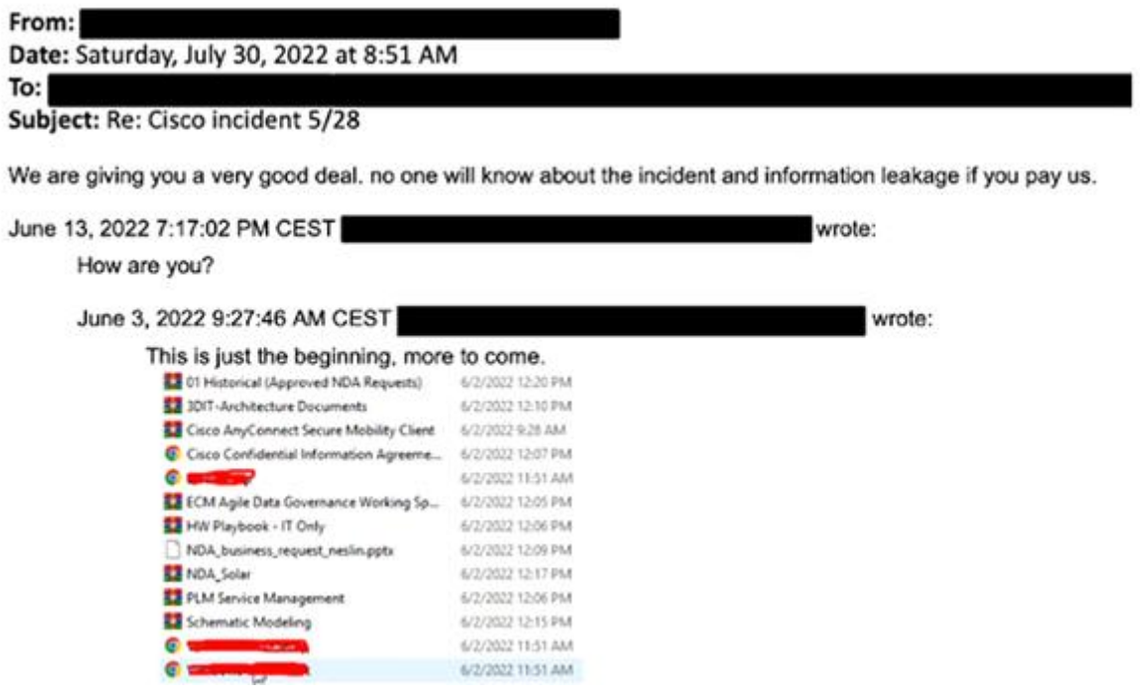
공격을 자세히 설명한 Cisco의 5월 분석에 따르면 공격자는 직원의 개인 Google 계정을 성공적으로 획득한 후 회사의 VPN에 대한 초기 액세스 권한을 얻었습니다. 이 공격자는 UNC2447 및 Lapsus$ 사이버 범죄 조직과 Yanluowang 랜섬웨어 그룹 모두에 대한 초기 액세스 브로커로 식별됩니다.

Yanluowang 범죄 조직은 비싱(Vishing)과 MFA 피로(MFA Fatigue)를 통해 공격을 시작했습니다. 비싱(Vishing)은 신뢰할 수 있는 지원 조직을 모방하기 위해 정교하게 설계된 일련의 보이스 피싱 공격이며 MFA 피로(MFA Fatigue)는 사용자가 요청을 수락하기를 바라는 희망을 품고 다중 요소 인증 요청을 반복적으로 푸시하는 공격입니다. 이 두 가지 공격을 조합하여 공격자는 대상 직원의 컨텍스트에서 VPN을 획득하고 권한을 상승하고 Cobalt Strike 및 Mimikatz와 같은 다양한 해킹 도구를 심었습니다. 또 향후 지속적인 연결을 위해 백도어 계정을 추가하기도 했습니다.

이 공격에서 공격자는 데이터 수집과 정찰을 위해 다양한 도구를 사용했는데, 여기에는 TeamViewer. LogMeIn과 같은 원격 액세스 도구, Mimikatz, Imppacket, PowerSpoilt 등의 공격 도구 및 기타 도구들이 포함됩니다. 그들은 또한 백도어 계정 추가하고 지속성 메커니즘을 설정했으며 ntdsutil.exe와 같은 LOLbin을 사용하여 NTDS 덤프를 실행했습니다.

그러나 공격자는 손상된 직원의 계정에 연결된 BOX 폴더 콘텐츠에서만 데이터를 유출할 수 있었습니다. Cisco는 공격자가 Active Directory에서 Box 폴더의 내용과 직원의 인증 데이터를 유출했지만 랜섬웨어가 배포되지는 않았으며 이 특정 사건이 비즈니스나 고객에게 영향을 주지는 않았다고 언급했습니다. 공격자는 아래와 같이 이메일을 통해 Cisco 경영진과 협상을 시도했습니다. Cisco의 기사는 해당 그룹이 내부 환경에서 제거된 후 회사 경영진과 이메일 통신을 시도했으며 최초 침해 후 몇 주 내에 액세스 권한을 회복하려 했으나, 이후의 모든 시도는 실패했다고 보고했습니다.

[그림 2] Cisco incident



From: [redacted]
Date: Saturday, July 30, 2022 at 8:51 AM
To: [redacted]
Subject: Re: Cisco incident 5/28

We are giving you a very good deal. no one will know about the incident and information leakage if you pay us.

June 13, 2022 7:17:02 PM CEST [redacted] wrote:

How are you?

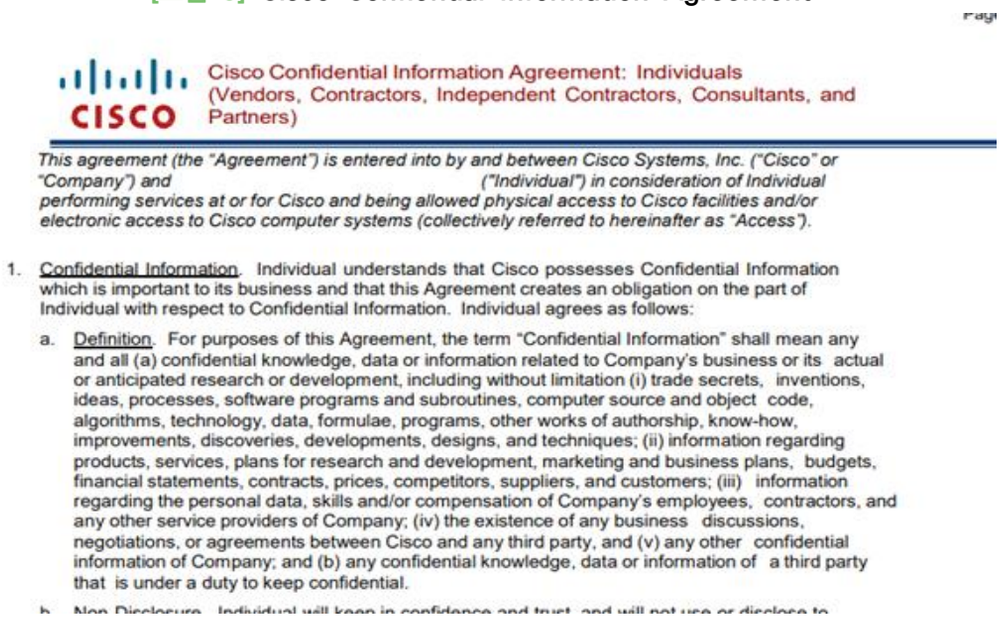
June 3, 2022 9:27:46 AM CEST [redacted] wrote:

This is just the beginning, more to come.

01 Historical (Approved NDA Requests)	6/2/2022 12:20 PM
3DIT-Architecture Documents	6/2/2022 12:10 PM
Cisco AnyConnect Secure Mobility Client	6/2/2022 9:28 AM
Cisco Confidential Information Agreeme...	6/2/2022 12:07 PM
[redacted]	6/2/2022 11:51 AM
ECM Agile Data Governance Working Sp...	6/2/2022 12:05 PM
HW Playbook - IT Only	6/2/2022 12:06 PM
NDA_business_request_neslin.pptx	6/2/2022 12:09 PM
NDA_Solar	6/2/2022 12:17 PM
PLM Service Management	6/2/2022 12:06 PM
Schematic Modeling	6/2/2022 12:15 PM
[redacted]	6/2/2022 11:51 AM
[redacted]	6/2/2022 11:51 AM

공격자는 CISCO에서 주요정보 유출에 대하여 인정하지 않자, 보안매체에 하기의 Cisco 내부 NDA자료를 증거로 제공합니다. 더불어 공격자들은 3,100개의 파일과 2.75GB의 데이터를 유출시켰고, 그 데이터는 비공개 계약, 데이터 덤프 및 엔지니어 자료라고 주장하였습니다. 공격자는 지속적으로 Cisco의 VMware vCenter 관리자 콘솔의 스크린샷을 공유했습니다. 그러나 Cisco는 해당 공격에는 소스 코드가 유출되었다는 증거가 없다고 말합니다.[4)]

[그림 3] Cisco Confiential Information Agreement



Cisco Confidential Information Agreement: Individuals (Vendors, Contractors, Independent Contractors, Consultants, and Partners)

This agreement (the "Agreement") is entered into by and between Cisco Systems, Inc. ("Cisco" or "Company") and ("Individual") in consideration of Individual performing services at or for Cisco and being allowed physical access to Cisco facilities and/or electronic access to Cisco computer systems (collectively referred to hereinafter as "Access").

1. Confidential Information. Individual understands that Cisco possesses Confidential Information which is important to its business and that this Agreement creates an obligation on the part of Individual with respect to Confidential Information. Individual agrees as follows:

   a. Definition. For purposes of this Agreement, the term "Confidential Information" shall mean any and all (a) confidential knowledge, data or information related to Company's business or its actual or anticipated research or development, including without limitation (i) trade secrets, inventions, ideas, processes, software programs and subroutines, computer source and object code, algorithms, technology, data, formulae, programs, other works of authorship, know-how, improvements, discoveries, developments, designs, and techniques; (ii) information regarding products, services, plans for research and development, marketing and business plans, budgets, financial statements, contracts, prices, competitors, suppliers, and customers; (iii) information regarding the personal data, skills and/or compensation of Company's employees, contractors, and any other service providers of Company; (iv) the existence of any business discussions, negotiations, or agreements between Cisco and any third party, and (v) any other confidential information of Company; and (b) any confidential knowledge, data or information of a third party that is under a duty to keep confidential.

   b. Non-Disclosure. Individual will keep in confidence and trust, and will not use or disclose to

4) https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

4. Cisco 침해 상세 분석

Cisco사의 Cisco Talos(위협 인텔리전스 팀)이 공유한 분석을 기반으로 공격자의 매 실행단계를 MITRE ATT&CK와 연계하여 설명합니다.

[그림 4] Cisco 침해 개요

[표 1] 실행 공격 및 관련 MITRE Technique

실행: Cisco 직원의 개인 Google 계정을 성공적으로 도용해서 Cisco VPN의 초기 액세스가 이루어졌습니다.

MITRE Technique	Attack ID	설 명
Credentials from Web Browsers	T1555.003	공격자는 대상 브라우저의 특정 파일을 읽어 웹 브라우저에서 자격 증명을 얻을 수 있습니다. 웹 브라우저는 일반적으로 웹 사이트 사용자 이름 및 암호와 같은 자격 증명을 저장하므로 나중에 수동으로 입력할 필요가 없습니다. 웹 브라우저는 일반적으로 자격 증명 저장소 내에 암호화된 형식으로 자격 증명을 저장합니다. 그러나 웹 브라우저에서 일반 텍스트 자격 증명을 추출하는 방법이 있습니다.

[표 2] 실행 공격 및 관련 MITRE Technique

실행: 공격자는 보이스 피싱(일명 "Vishing") 및 다단계 인증 반복으로 인한 피로(MFA fatigue)를 비롯한 다양한 기술을 사용하여 다단계 인증(MFA)을 우회했습니다. MFA용으로 일련의 새 장치를 등록하고 Cisco VPN에 성공적으로 인증했습니다.

MITRE Technique	Attack ID	설 명
Phishing(Vishing)	T1204	공격자는 또한 원격 액세스 소프트웨어 활성화, 공격자에게 시스템 직접 제어 허용, 사용자 실행을 위한 맬웨어 다운로드 및 실행과 같은 작업을 수행하도록 사용자를 속일 수 있습니다 . 예를 들어 기술 지원 사기는 피싱, 비싱 또는 다양한 형태의 사용자 상호 작용을 통해 촉진될 수 있습니다.
Multi-Factor Authentication Request Generation	T1621	공격자는 사용자에게 MFA 푸시 알림, SMS 메시지 및 전화 통화를 퍼붓기 위해 로그인 시도를 계속 반복할 수 있으며, 잠재적으로 사용자가 "MFA 피로"에 대한 응답으로 인증 요청을 수락하게 될 수 있습니다.

[표 3] 실행 공격 및 관련 MITRE Technique

실행: 시스템 침투하자마자 공격자는 기본 제공된 Windows 유틸리티를 사용하여 해당 시스템에서 사용자 및 그룹 구성원 구성, 호스트 이름, 및 사용자 계정 컨텍스트를 식별하고 Active Directory(AD) 환경을 열거하기 시작했습니다.

MITRE Technique	Attack ID	설 명
File and Directory Discovery	T1083	공격자는 파일 및 디렉토리를 열거하거나 호스트 또는 네트워크 공유의 특정 위치에서 파일 시스템 내의 특정 정보를 검색할 수 있습니다. 공격자는 자동 검색 중에 파일 및 디렉터리 검색 정보를 사용하여 공격자가 대상을 완전히 감염시키거나 특정 작업을 시도하는지 여부를 포함하여 후속 행동을 형성할 수 있습니다.

[표 4] 실행 공격 및 관련 MITRE Technique

실행: 공격자는 Citrix 환경으로 측면 이동하여 일련의 Citrix 서버를 감염시키고 결국 DC(도메인 컨트롤러)에 대한 권한 있는 액세스를 획득합니다. 권한을 얻은 후 "ntdsutil.exe" 명령을 사용하여 NTDS 덤프를 실행했습니다.

MITRE Technique	Attack ID	설 명
OS Credential Dumping: NTDS	T1003.003	공격자는 자격 증명 정보를 훔치고 장치, 사용자 및 액세스 권한과 같은 도메인 구성원에 대한 기타 정보를 얻기 위해 Active Directory 도메인 데이터베이스에 액세스하거나 복사본을 만들려고 시도할 수 있습니다. 기본적으로 NTDS 파일(NTDS.dit)은 %SystemRoot%\NTDS\Ntds.dit 도메인 컨트롤러에 있습니다.

[표 5] **실행 공격 및 관련 MITRE Technique**

실행: 공격자는 전체 환경에서 권한 있는 인증 및 측면 이동을 위해 시스템 계정을 활용하고 기본 제공된 Windows "net.exe" 명령을 사용하여 시스템에 "z"라는 Administrators 그룹의 사용자를 생성하고 ADfind 또는 secretsdump와 같은 추가 유틸리티를 실행했습니다. 또한 손상된 Windows 엔드포인트의 SAM 데이터베이스를 비롯한 레지스트리 정보를 추출하려고 시도하였습니다.

MITRE Technique	Attack ID	설 명
Create Account: Local Account	T1098.005	공격자는 피해자 시스템에 대한 액세스를 유지하기 위해 로컬 계정을 생성할 수 있습니다. 로컬 계정은 사용자, 원격 지원, 서비스가 사용하거나 단일 시스템 또는 서비스에서 관리하기 위해 조직에서 구성하는 계정입니다. 액세스 수준이 충분하면 net user /add명령을 사용하여 로컬 계정을 만들 수 있습니다.
OS Credential Dumping: Security Account Manager	T1003.002	공격자는 인메모리 기술이나 SAM 데이터베이스가 저장된 Windows 레지스트리를 통해 보안 계정 관리자(SAM) 데이터베이스에서 자격 증명 자료를 추출하려고 시도할 수 있습니다. SAM은 일반적으로 net user명령으로 찾은 호스트의 로컬 계정을 포함하는 데이터베이스 파일입니다.

[표 6] **실행 공격 및 관련 MITRE Technique**

실행: 공격자는 일부 피해자 엔드포인트에서 Mimikat의 MiniDump를 사용하여 LSASS 덤프를 실행했습니다. 그들은 또한 "wevtutil.exe" 유틸리티를 활용하여 시스템에서 생성된 이벤트 로그를 식별하고 지웠습니다.

MITRE Technique	Attack ID	설 명
OS Credential Dumping: LSASS Memory	T1003.001	공격자는 LSASS(Local Security Authority Subsystem Service)의 프로세스 메모리에 저장된 자격 증명 자료에 액세스를 시도할 수 있습니다. 사용자가 로그온하면 시스템은 LSASS 프로세스 메모리에 다양한 자격 증명 자료를 생성하고 저장합니다.
Indicator Removal on Host: Clear Windows Event Logs	T1070.001	공격자는 Windows 이벤트 로그를 삭제하여 침입 활동을 숨길 수 있습니다. Windows 이벤트 로그는 컴퓨터의 경고 및 알림에 대한 기록입니다. 시스템 정의 이벤트 소스는 시스템, 응용 프로그램 및 보안의 세 가지이며 5가지 이벤트 유형(오류, 경고, 정보, 성공 감사 및 실패 감사)이 있습니다.

[표 7] 실행 공격 및 관련 MITRE Technique

실행: 공격자는 RDP로 시스템에 액세스할 수 있도록 호스트 기반 방화벽 구성을 수정하여 RDP(원격 데스크톱 프로토콜) 및 Citrix를 활용했습니다. 그들은 TeamViewer, LogMeIn, Cobalt Strike, PowerSploit, Mimikatz 및 Imppacket를 비롯한 추가 원격 액세스 도구를 설치했습니다. 또한 맞춤형 백도어 계정을 추가하고 지속성 메커니즘을 설정했습니다.

MITRE Technique	Attack ID	설 명
Impair Defenses: Disable or Modify System Firewall	T1562.004	공격자는 네트워크 사용을 제한하는 제어를 우회하기 위해 시스템 방화벽을 비활성화하거나 수정할 수 있습니다. 변경으로 인해 전체 메커니즘이 비활성화되고 특정 규칙이 추가, 삭제 또는 수정될 수 있습니다.
Remote Access Software	T1219	공격자는 Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin 등과 같은 합법적인 데스크톱 지원 및 원격 액세스 소프트웨어를 사용하여 네트워크 내의 대상 시스템에 대한 대화형 명령 및 제어 채널을 설정할 수 있습니다.
Create Account: Local Account	T1136.001	공격자는 피해자 시스템에 대한 액세스를 유지하기 위해 로컬 계정을 생성할 수 있습니다. 로컬 계정은 사용자, 원격 지원, 서비스가 사용하거나 단일 시스템 또는 서비스에서 관리하기 위해 조직에서 구성한 계정입니다.

[표 8] 실행 공격 및 관련 MITRE Technique

실행: 공격자는 명령 및 제어(C2) 서버로부터 명령을 받아 Windows 명령 프로세서를 통해 실행되는 일련의 페이로드를 엔드포인트에 떨어뜨렸습니다.

MITRE Technique	Attack ID	설 명
Command and Control	TA0011	공격자는 감염된 시스템과 통신하여 제어하려고 합니다. 명령 및 제어 서버는 공격자가 피해자 네트워크 내에서 자신이 제어하는 시스템과 통신하는 데 사용할 수 있는 기술로 구성됩니다.
Indicator Removal on Host: File Deletion	T1070.004	공격자는 침입 활동으로 인해 남겨진 파일을 삭제할 수 있습니다. 악성 코드, 도구 또는 공격자가 시스템에 떨어뜨리거나 생성한 기타 기본이 아닌 파일(예: Ingress Tool Transfer)은 네트워크 내에서 수행된 작업과 방법을 나타내는 추적을 남길 수 있습니다. 이러한 파일의 제거는 침입 중에 발생하거나 공격자의 흔적을 최소화하기 위한 침입 후 프로세스의 일부로 발생할 수 있습니다.

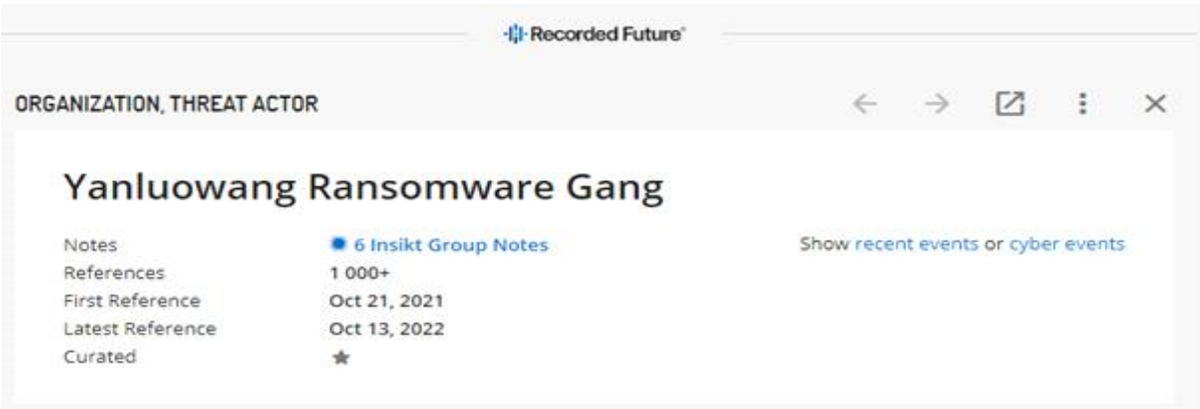
[표 9] 실행 공격 및 관련 MITRE Technique

실행: 공격자가 대상 환경에서 정보를 유출하려고 시도했습니다. 이 공격에서 유출된 데이터에는 감염된 직원 장치에 있는 Box 폴더 콘텐츠와 Active Directory의 직원 인증 데이터가 포함되어 있었습니다.

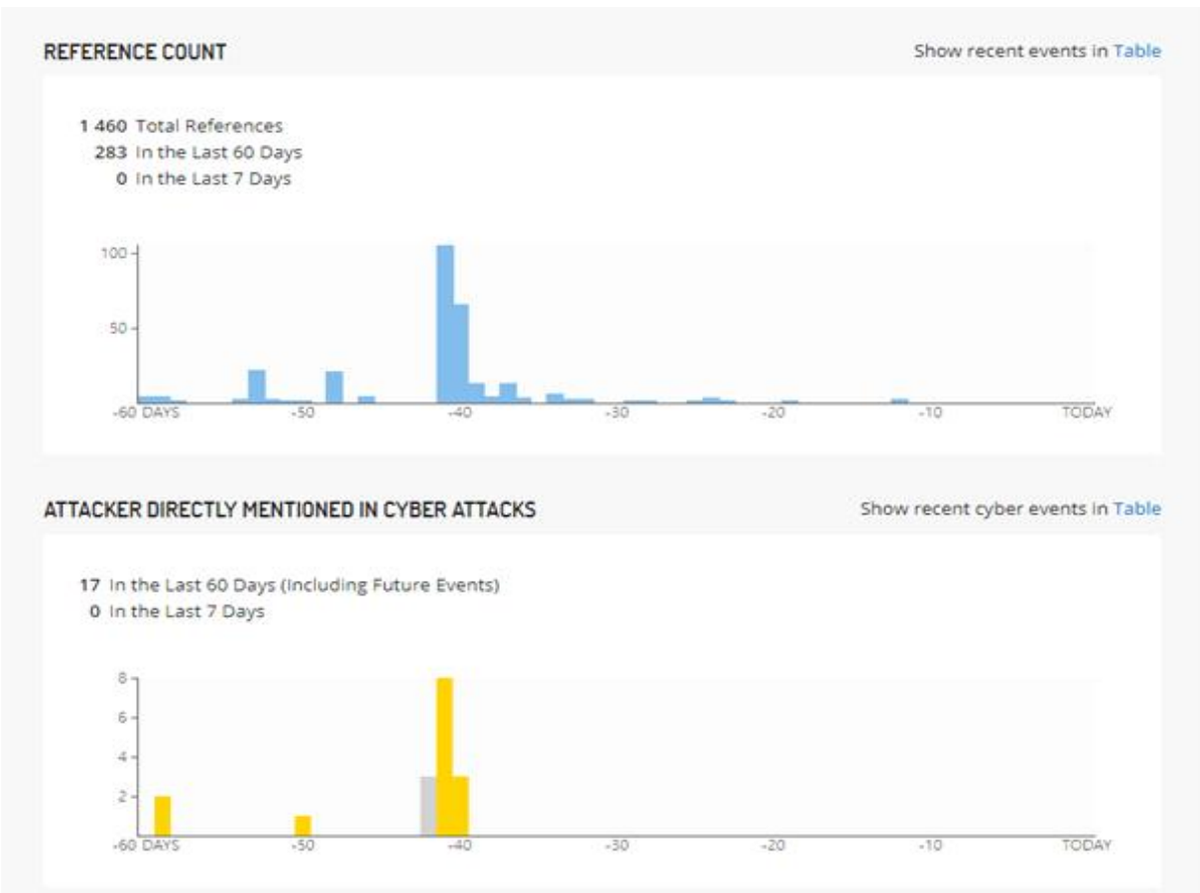
MITRE Technique	Attack ID	설 명
Exfiltration Over C2 Channel	T1041	공격자는 기존 명령 및 제어 채널을 통해 데이터를 유출하여 데이터를 훔칠 수 있습니다. 도난당한 데이터는 명령 및 제어 통신과 동일한 프로토콜을 사용하여 일반 통신 채널로 인코딩됩니다.

Appendix
Yanluownag Ransomware Gang 관련 지표

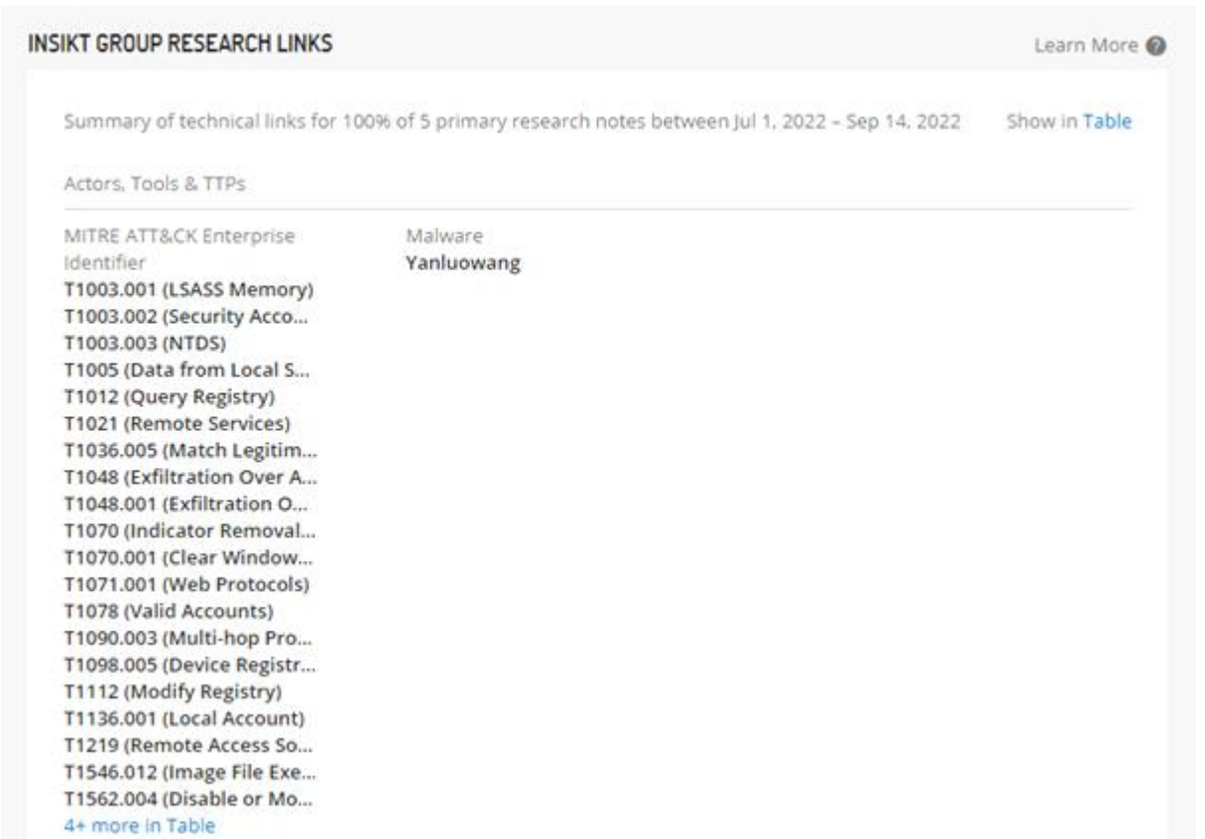
[그림 5] 종합 지표



[그림 6] 공격 그룹 관련 이벤트: 다크웹 포함



[그림 7] 공격자 TTP 분석지표



[그림 8] 종합 지표


CONTEXT
Show all entities in Table
Company 6 of 71 Risk
Twitter 109 87
The Hacker News 108 37
Twitter Communicatio... 104 0
Shenzhen Micro Twitter Netwo... 89
Walmart 68 94
Google 59 99
Show in Table
Hash 6 of 10 Risk
184a2570d71eedc3c77b6... 4 72
2fc5bf9edcfa19d48e2353... 4 68
542c9da985633d027317e... 4 71
61176a5756c7b953bc31e... 4 66
753952aed395ea845c52e... 4 67
8df89eef51cdf43b2a992a... 4 67
Show in Table
Email Address Risk
costacancordia@protonmail.com 2
noreply@blogger.com 2
thenewoil@freeradical.zone 1
Show in Table
Domain 6 of 23 Risk
cisco-help.cf 2 72
cisco-helpdesk.cf 2 72
ciscovpn1.com 2 67
ciscovpn2.com 2 67
ciscovpn3.com 2 66
devcisco.com 2 68
Show in Table
Technology 6 of 31 Risk
Multi Factor Authentication 63
Dark Web 31
Internet 15
Computer Networking 12
Hyper Text Transfer Protocol Se... 11
VPN 7
Show in Table
IP Address 6 of 71 Risk
104.131.30.201 2 33
108.191.224.47 2 29
131.150.216.118 2 28
134.209.88.140 2 29
138.68.227.71 2 31
139.177.192.145 2 34
Show in Table
Organization 6 of 20 Risk
UNC2447 50
Lapsus$ Group 47
Cyber Threat Intelligence 6 0
DeathStalker 3
Conti Gang 3
Hive Ransomware Group 3
Show in Table
Country 6 of 9 Risk
United States 14
Russia 8
India 3
Denmark 3
Germany 2
China 2
Show in Table
Malware 6 of 11 Risk
Yanluowang Ransomware 117
Cobalt Strike Offensive Security ... 3
Conti Ransomware Ransomware 3
Cuba Ransomware Ransomware 3
BazarCall Phishing Kit 3
Hive Ransomware Ransomware 3
Show in Table
Malware Category Risk
Ransomware 287
Backdoor 11
Remote Access Trojan 3
Phishing Kit 3
Offensive Security Tools (OST) 3
Stealware 2
Show in Table
Threat Actor 6 of 13 Risk
UNC2447 50
Lapsus$ Group 47
Hackers 4
CyberCriminal 4
DeathStalker 3
Conti Gang 3
Show in Table
Username 6 of 100+ Risk
@serghei on Twitter 41
@BleepinComputer on Twitter 39
@TheHackersNews on Twitter 12
@vxunderground on Twitter 10
@MgdHermes on Twitter 10
@Gi7w0rm on Twitter 9
Show in Table
Attack Vector 6 of 8 Risk
Phishing 60
Cyberattack 15
Vishing 5
Kerberoasting 3
Account Hijacking 3
Social Engineering 2
Show in Table
Product 6 of 17 Risk
Twitter Media 104
Twitter Blue Labs 104
Cisco VPN 5
SysInternals 4
PsExec 4
Google Sites 3
Show in Table

Reference

- Watchtower report(SentinelOne)
- Threat Intelligence(Recorded Future)
- https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

[표 10] 공격자 관련 Hash

Type	Value
Hash	8e5733484982d0833abbd9c73a05a667ec2d9d005bbf517b1c8cd4b1daf57190
Hash	753952aed395ea845c52e3037f19738cfc9a415070515de277e1a1baeff20647
Hash	bb62138d173de997b36e9b07c20b2ca13ea15e9e6cd75ea0e8162e0d3ded83b7
Hash	184a2570d71eedc3c77b63fd9d2a066cd025d20ceef0f75d428c6f7e5c6965f3
Hash	2fc5bf9edcfa19d48e235315e8f571638c99a1220be867e24f3965328fe94a03
Hash	542c9da985633d027317e9a226ee70b4f0742dcbc59dfd2d4e59977bb870058d
Hash	99be6e7e31f0a1d7eebd1e45ac3b9398384c1f0fa594565137abb14dc28c8a7f
Hash	eb3452c64970f805f1448b78cd3c05d851d758421896edd5dfbe68e08e783d18
Hash	8df89eef51cdf43b2a992ade6ad998b267ebb5e61305aeb765e4232e66eaf79a
Hash	61176a5756c7b953bc31e5a53580d640629980a344aa5ff147a20fb7d770b610

[표 11] 공격자 관련 Domain

Type	Value
InternetDomainName	primecisco.com
InternetDomainName	devciscoprograms.com
InternetDomainName	ciscovpn2.com
InternetDomainName	kazaboldu.net
InternetDomainName	pwresetcisco.com
InternetDomainName	cisco-helpdesk.cf
InternetDomainName	devcisco.com
InternetDomainName	mycisco.cf
InternetDomainName	ciscovpn3.com
InternetDomainName	mycisco.gq
InternetDomainName	helpzonecisco.com
InternetDomainName	mycisco-helpdesk.ml
InternetDomainName	ciscovpn1.com
InternetDomainName	cisco-help.cf

[표 12] 공격자 관련 IP Address

Type	Value	Type	Value
IP Address	185.220.101.65	IP Address	65.188.102.43
IP Address	104.131.30.201	IP Address	167.99.160.91
IP Address	172.58.220.52	IP Address	185.220.101.15
IP Address	139.177.192.145	IP Address	52.154.0.241
IP Address	45.32.141.138	IP Address	174.205.239.164
IP Address	185.220.101.16	IP Address	94.142.241.194
IP Address	45.227.255.215	IP Address	73.153.192.98
IP Address	64.227.0.177	IP Address	139.60.161.99
IP Address	161.35.137.163	IP Address	108.191.224.47
IP Address	162.33.177.27	IP Address	143.198.131.210
IP Address	185.220.101.10	IP Address	178.128.171.206
IP Address	45.61.136.83	IP Address	64.4.238.56
IP Address	139.60.160.20	IP Address	176.59.109.115
IP Address	195.149.87.136	IP Address	185.220.101.34
IP Address	45.32.228.189	IP Address	162.33.179.17
IP Address	82.116.32.77	IP Address	159.65.246.188
IP Address	131.150.216.118	IP Address	165.227.219.211
IP Address	66.42.97.210	IP Address	138.68.227.71
IP Address	45.145.67.170	IP Address	45.61.136.207
IP Address	185.220.101.79	IP Address	87.251.67.41
IP Address	185.220.101.45	IP Address	74.119.194.4
IP Address	162.33.178.244	IP Address	166.205.190.23
IP Address	134.209.88.140	IP Address	185.220.100.244
IP Address	185.220.101.73	IP Address	74.119.194.203
IP Address	172.58.239.34	IP Address	67.171.114.251
IP Address	76.22.236.142	IP Address	192.241.133.130
IP Address	185.220.101.13	IP Address	143.198.110.248
IP Address	45.55.36.143	IP Address	68.46.232.60
IP Address	24.6.144.43	IP Address	185.220.101.6
IP Address	165.232.154.73	IP Address	185.220.101.20
IP Address	46.161.27.117	IP Address	5.165.200.7
IP Address	68.183.200.63	IP Address	45.61.136.5
IP Address	172.56.42.39	IP Address	194.165.16.98
IP Address	45.32.228.190	IP Address	185.220.101.2

2022년 주요 랜섬웨어 및 대응방안

안랩, 김건우 실장, keonwoo.kim@ahnlab.com

2022년에도 다수의 랜섬웨어가 여전히 활발하게 활동하고 있고 많은 피해자를 양산하고 있다.
따라서 최근의 랜섬웨어들이 유포되는 경로를 알아보고 이에 대한 대비 방안을 고민해보고자 한다.

1. 국내 유포 중인 주요 랜섬웨어

1) Magniber

Magniber는 주로 타이포스쿼팅(typosquatting) 공격으로 알려진 도메인의 오탈자로 인해 잘못 방문하는 사이트를 통해 유포되거나, 불법 다운로드사이트, 광고 링크를 통해 유포되고 있다. 불특정 다수를 타겟으로 하고 있으며, 수많은 변형을 양산하고 있어 국내 개인을 포함해 많은 감염 사례가 발생하고 있다.

최근 몇년간 주로 Internet Explorer의 취약점을 이용해서 유포되었으나 최근에는 Edge, Chrome 브라우저를 통해서도 유포가 되고 있다. Internet Explorer의 취약점을 이용하는 경우 유포 사이트에 접속하는것 만으로도 감염이 되지만 Edge와 Chrome의 경우는 다운로드가 이루어지지만 자동 실행은 되지 않으므로 Edge, Chrome, OS 등의 업데이트 파일인 것처럼 위장하여 사용자의 클릭을 유도한다.

2) LockBit 3.0

LockBit 랜섬웨어는 이메일을 통해 유포되고 있으며, 저작권 사칭, 입사 지원서 등으로 위장한 이메일을 통해 유포되고 있다. 첨부파일에는 문서로 위장한 실행파일을 비밀번호로 압축한 압축파일이나, External Link를 포함한 docx 문서 파일이 포함되어 사용자가 문서를 보기위해 실행파일을 실행시키거나 문서 내의 VBA 매크로를 실행하도록 유도한다.

국내 고객사의 Microsoft Exchange Server 의 취약점을 이용해 침투하고 계정 정보를 탈취한 후 시스템을 완전히 장악한 후 다수의 시스템에 이 랜섬웨어를 실행시킨 경우도 확인되었다.

LockBit 공격자는 이메일이나 취약점을 통해 초기 침투에 성공한 후 백도어 설치, 내부 시스템을 파악, 계정 정보 획득, 측면이동, 정보유출 후 랜섬웨어 감염으로 공격을 완성하게 되며 피해자가 복호화에 대한 대가를 지불하지 않을 경우 LockBit 블로그를 통해 유출한 데이터를 공개하고 있다.

3) Gwisin

최근 국내 기업을 대상으로 감염 사례가 여러 건 확인되었다.

이 랜섬웨어는 msi 형태이며, 실행 시 인자로 특별한 값을 입력해야 실행이 가능하며 암호화된 파일의 확장자가 감염대상 기업의 약자로 변경된다. 또한 안전모드로 재부팅 후 암호화를 진행하여 랜섬웨어 행위를 차단하는 보안 솔루션을 우회한다.

이러한 특징은 공격 대상을 특정하고 계정과 권한 상승 등 시스템을 장악한 후에 최종적으로 수행하는 공격 단계로서 랜섬웨어가 사용되는 것으로 전형적인 APT 공격의 형태이다.

4) FARGO

FARGO 랜섬웨어는 GlobImposter 랜섬웨어와 함께 관리가 취약한(unsecured) MS-SQL 서버를 통해 유포되고 있다.

취약점이 패치되지 않은 시스템에 대한 취약점 공격이나 부적절하게 계정 정보를 관리하고 있는 시스템들에 대한 무차별 대입 공격(Brute Forcing)과 사전 공격(Dictionary Attack)이 주로 사용되는 것으로 보인다.

공격에 성공하면 MS-SQL 프로세스에 의해 cmd.exe 및 powershell.exe를 거쳐 닷넷으로 제작된 악성파일을 생성하고 추가 파일을 다운로드 받는다.

랜섬웨어 행위는 윈도우 정상 프로그램인 AppLaunch.exe에 인젝션하여 실행되며 볼륨 섀도우 복사본을 삭제한 후 MS-SQL 프로세스를 종료하고 암호화를 진행한다.

2. 랜섬웨어 초기 침투 경로

1) 이메일 (Spear Phishing)

사회공학적 기법을 이용해 불특정 다수 또는 특정 대상에게 이메일의 첨부파일을 열어보거나 링크를 방문하게 하고 있으며 이것은 악성코드 감염과 공격의 시작점이 되는 좋은 수단으로 활용되고 있다.

국내를 타겟으로 공격을 하는 경우 한국어에 능숙할 뿐만 아니라 이메일과 첨부된 문서 내용이 너무 그럴 듯해서 쉽게 속을 수 있다.

2) 웹 브라우저 (Watering hole)

과거 Internet Explorer의 각종 취약점을 통해 랜섬웨어가 유포되었으나 지금도 여전히 Edge, Chrome 등의 브라우저를 통해 랜섬웨어가 유포되고 있다.

단순히 랜섬웨어를 다운로드 받고 클릭을 유도하는 것뿐만 아니라 사이트와 상호작용하는 일부 취약한 프로그램이 설치되어 있다면 사이트에 방문하는 것만으로도 랜섬웨어에 감염될 수 있다.

3) 소프트웨어, OS 취약점 (Application Vulnerability)

원격 코드 실행이 가능한 취약점이 공개되면 마치 유행을 따르듯이 해당 공격을 이용하는 공격들이 급증하곤 한다. 또한 공개되지 않은 취약점들도 공격자들 사이에 은밀하게 공유되고 거래되는 것으로 보인다.

물론 최신의 취약점을 빠르게 조치하는 것이 어려운 만큼 공격자들도 새로운 취약점을 찾는게 항상 쉬운 일은 아닐 것이다. 그래서 공격자는 철 지난 취약점이지만 여전히 오래된 취약한 버전을 사용하는 대상을 물색하는 방안을 선택하기도 한다. 특정 솔루션이 1년 전에 취약점이 공개되고 보안 패치가 나왔으나 여전히 그 취약한 버전을 사용하고 있다가 피해가 발생한 경우도 확인되고 있다.

최근 국내 타겟으로 활동 중인 공격 그룹이 많이 활용하는 취약점 공격 솔루션들은 다음과 같으며 이외에도 사용 중인 모든 솔루션에 대한 취약점을 모니터링하고 업데이트를 해야 한다.

- Microsoft Exchange Server
- Microsoft MS-SQL Server
- DreamSecurity MagicLine
- intech INISAFE Web Ex Client
- Apache Log4j

4) 관리 취약점 (IT Management)

어떤 공격은 단순히 암호를 무작위로 대입하는 것만으로 공격에 성공하기도 한다. 만일 asdfqwer 같은 암호를 사용하고 있다면 당장 암호를 바꿔야한다.

불필요한 공유폴더를 통해 랜섬웨어에 의해 대량으로 파일 암호화가 되어버리거나 모든 서버의 암호가 동일해서 여러 시스템이 한 번에 장악당하기도 한다.

5) 공급망 (Supply Chain)

업무 시스템에는 각종 업무용 소프트웨어와 보안 프로그램을 설치하고 사용한다. 금융 사이트 이용을 위해 설치하는 여러 프로그램들도 업무 시스템에 동작하고 있을 수 있다.

이들 소프트웨어의 업데이트 서버가 침해당하거나 취약점이 포함된 경우 종종 업데이트 서버나 중계서버 또는 솔루션 자체의 웹서비스를 악용하여 악성코드가 유포될 수 있다.

3. 최근 랜섬웨어 감염 사례

최근 확인된 몇 가지 랜섬웨어 감염 사례를 보면 다음과 같다.

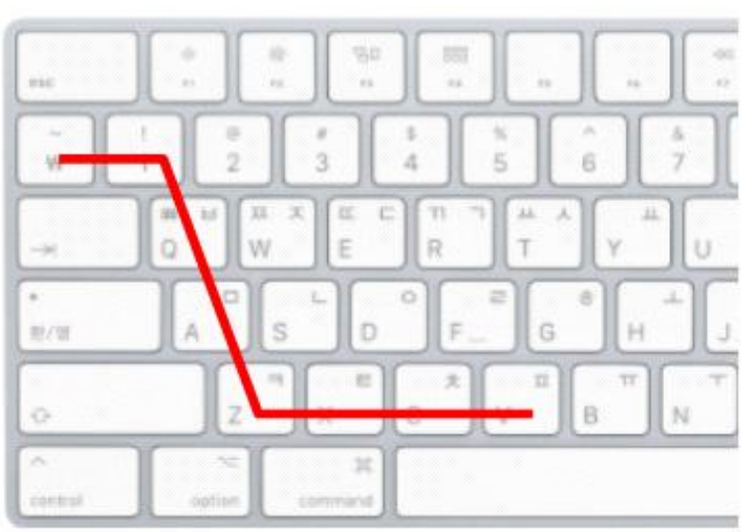
1) Lockis 랜섬웨어 감염 사례

A업체는 작년 11월경 다수의 서버가 Lockis 랜섬웨어에 감염되었다.

공격자는 Administrator 계정으로 RDP 접속 후 백신을 언인스톨하고 해킹툴 및 랜섬웨어를 복사하고 다수의 시스템에 접속해서 랜섬웨어를 실행했다.

공격자가 Administrator 계정 비밀번호를 어떻게 알아냈는지 알 수는 없으나 당시 비밀번호는 '1qazxcv'로 확인되었다. 이 비밀번호는 영문자, 숫자, 특수문자가 모두 포함돼 복잡도 기준은 만족시켰으나 키보드 상 연속된 위치에 존재하고 있어서 안전하지 않다. 그리고 이 비밀번호를 1~2년 동안 변경하지 않았으며, 여러 시스템에 동일한 비밀번호가 설정되어 있었다.

[그림 1] 키보드 상 연속된 위치의 비밀번호인 '1qazxcv'



해당 업체는 Microsoft ActiveDirectory를 운영중이었으나 피해 시스템들은 모두 로컬 Administrator 계정이 활성화 되어있어 로컬 Administrator 계정으로 RDP 접속이 가능한 상황이었다.

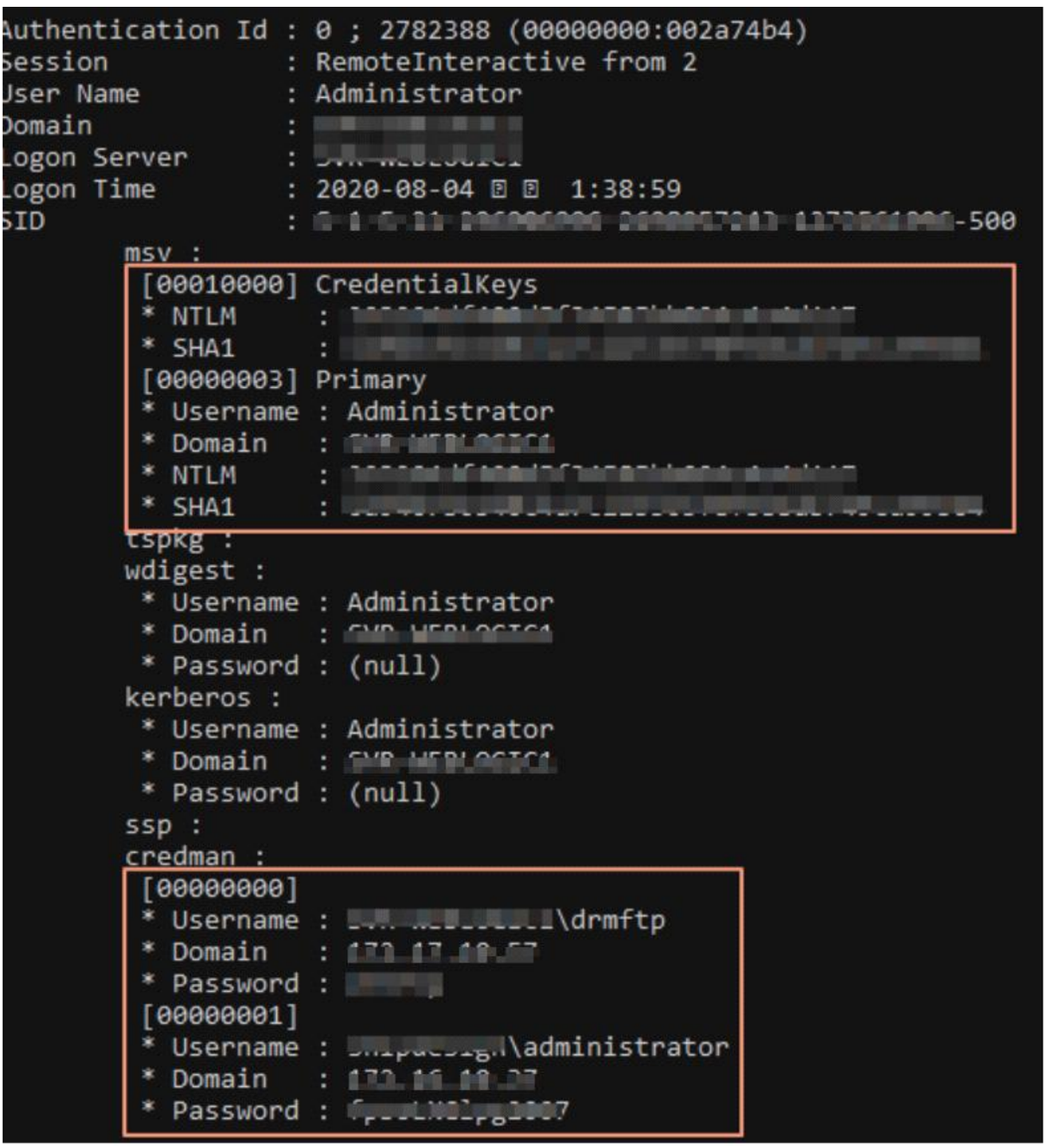
2) Darkside 랜섬웨어 감염 사례

B업체는 올해 1월에 기업 내부 다수 시스템이 Darkside 랜섬웨어에 감염되는 피해가 발생했다.

사용된 Darkside 랜섬웨어는 DC에서 동작 시 그룹 정책을 이용해 랜섬웨어를 전파시키는 것으로 분석됐다. 해당 업체는 DC 서버를 가상환경에서 운영하고 있어서 전파 과정에서 가상환경을 운영하는 시스템이 손상되어 감염된 DC 서버 이미지는 확보할 수 없었다.

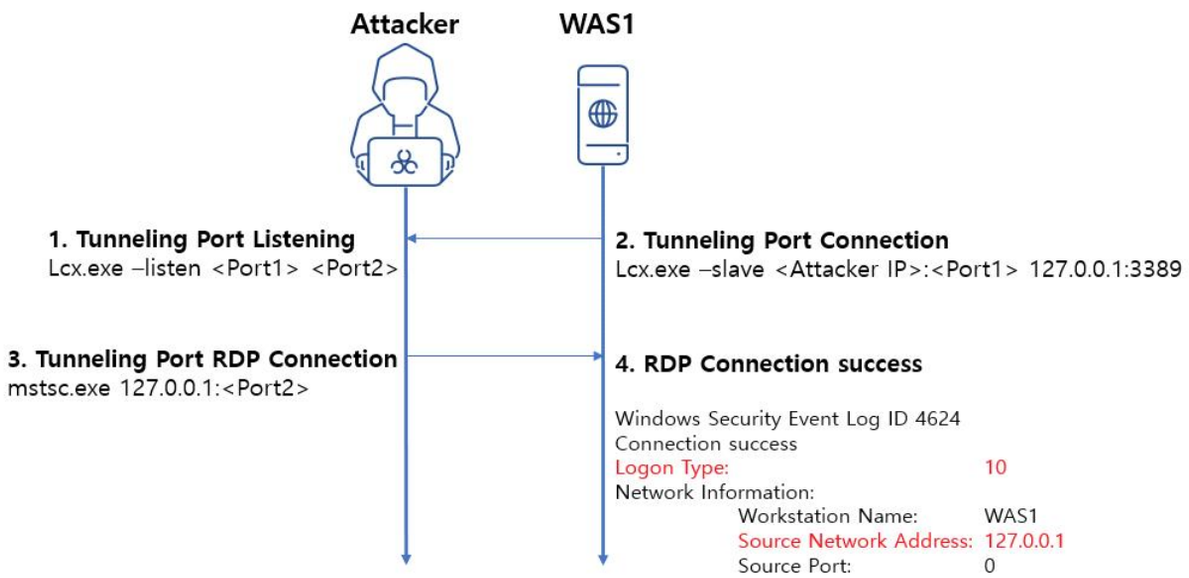
그러나 랜섬웨어 감염 일주일 전에 WebLogic 서버가 WebShell에 감염되었음을 확인하였으며 이미 2019년부터 코인마이너와 정보 수집 악성코드 실행 이력이 있었다. 해당 서버의 관리자 계정 비밀번호는 유추하기 쉬운 형태였으며 2018년 10월 이후 변경된 적이 없어 사전 공격 또는 다른 시스템에서 계정 탈취 악성코드를 이용해서 얻은 정보를 이용한 것으로 보인다.

[그림 2] 공격자가 탈취한 lsass.dmp에서 추출한 계정 정보(ID, 평문 PW, NTLM Hash)



이후에 터널링 도구 Lcx.exe를 이용해서 RDP에 접속하였는데, Reverse connection으로 공격자의 C2 서버에 연결한 후 이 연결을 통해 RDP 접속을 하여 방화벽을 우회했다.

[그림 2] Lcx.exe를 이용한 RDP 통신 과정



이 업체 역시 유추 가능한 관리자 비밀번호를 여러 시스템에 동일하게 사용하고 있었으며, 내부 주요 서버가 외부 인터넷에 접근이 가능하여 reverse connection 공격에 취약하였다.

3) LockBit 3.0 랜섬웨어 감염 사례

C업체는 올해 7월에 LockBit 3.0 랜섬웨어에 감염되는 피해가 발생했다. 이 업체는 Microsoft Exchange Server의 취약점을 통해 Webshell이 설치되었다. Microsoft Exchange Server는 당시에 최신 버전이었으나 Zero-day 취약점이 이용되어 침해가 발생한 것으로 추정되었다.

[그림 3] MicroSoft Exchange Server에 의해 생성된 WebShell 추정 파일

Name	Full path	Size	Created
.. = owa (113)	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa	2,735,617	2017/12/14 14:41:57.983
. = auth (108)	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth	2,708,087	2021/03/19 23:56:24.840
aBcl32M.Hj11yV10X	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth₩aBcl32M.Hj11yV...	3,547	2022/07/21 22:43:49.004
y7gm0c4.Hj11yV10X	₩ExchSvr₩V15₩FrontEnd₩HttpProxy₩owa₩auth₩y7gm0c4.Hj11yV...	365	2022/07/21 22:43:49.005

이후에 Mimikatz 악성코드를 이용해 시스템 계정을 탈취하였고 Plink를 이용해 터널링 연결을 하고 RDP 접속을 하였다.

다음 단계로 NetScan으로 다른 시스템을 검색하고 Active Directory 정보를 획득하며 전체 시스템을 장악하는데 6일이 소요되었으며 이 과정에서 다량의 데이터를 유출하였고 7일째 되는 날 랜섬웨어를 유포하여 수백대가 감염되었다.

4. 랜섬웨어 대응 방안

공격자는 랜섬웨어의 효과를 극대화하기 위해 초기 침투 후 내부 시스템을 장악하고 권한 획득과 많은 시스템에 대한 접근을 시도하는 경우가 많다. 따라서 침투 경로를 방어하는 것 뿐만 아니라 내부 시스템에 대한 관리를 철저히 한다면 피해를 최소화할 수 있다.

1) 불필요 시스템에 대한 외부 노출 최소화

업무 시스템과 주요 시스템들을 외부 인터넷으로부터 분리하는 것은 강력하고 효과적인 보호조치이다. 이것은 공격자의 공격 면적을 줄일 뿐 아니라 사용자의 부주의로 인한 의도치 않은 악성코드 감염이나 정보 탈취 가능성을 줄일 수 있다.

외부에서 접근할 필요가 없는 시스템에 대한 공인 IP 부여를 제한하고, 방화벽을 통해 최소한의 접근만을 허용해야 한다.

RDP 접속 등을 위한 reverse connection 공격도 일반적으로 방화벽의 outbound 정책을 강화할 필요가 있다.

2) DMZ 내 시스템 취약점 점검

외부에서의 접근이 허용되는 시스템은 보다 높은 보안 요구사항을 만족해야 한다.

이러한 시스템은 수시로 공격시도가 발생하게되며 이 중 하나 얻어 걸리면 최악의 상황으로 이어질 수도 있다. 시스템 취약점 점검도구와 망 구성에 대한 검토를 통해 보안성에 대한 검증을 철저하게 할 필요가 있다.

3) 계정 및 비밀번호 관리

로컬 Administrator 계정 등 불필요한 계정은 삭제하고 비밀번호 관리를 강화한다. 비밀번호는 시스템별로 서로 다르게 설정해야하며, 최대 사용기간을 3개월 이하로 설정하고 정기적으로 변경한다. 또한 관리자 권한 계정의 인증 이력은 반드시 모니터링해야 한다.

탈취된 VPN을 계정을 이용한 내부망 접근 사례도 있으므로 주기적으로 VPN 계정 비밀번호를 변경하도록 한다.

4) 보안 솔루션 사용

시스템의 요구사항과 기업 환경에 맞는 보안 솔루션을 도입하고 적절하게 운영한다.

백신은 항상 최신 버전으로 업데이트를 해야하며 각 보안 솔루션이 정상적으로 작동 중인지 모니터링한다. 공격자는 자신이 사용하는 공격기법과 툴이 보안 솔루션에 의해 차단되는 것을 막기 위해 우선적으로 보안 솔루션을 중단시키거나 삭제하는 등 무력화하기 위해 노력한다.

5) 중요 데이터 및 로그 백업

랜섬웨어에 감염되었을 때 백업된 데이터가 없다면 복구는 어렵다고 보아야 한다. 만일 공격자의 요구사항을 들어준다고 해도 공격자가 약속을 지킨다는 보장도 없다. OS에서 제공하는 볼륨 섀도 복사본은 대부분의 랜섬웨어가 최우선적으로 삭제하고 있어서 소용없을 가능성이 높다.

랜섬웨어 감염의 경우도 재난 발생 시와 같이 백업된 데이터와 깨끗한 머신 이미지로 복구하여 빠르게 시스템 가용성을 확보할 수 있도록 대비한다. 또한 중요 시스템의 로그를 정기적으로 백업하면 문제가 발생했을 때 장기적으로 발생한 APT 공격에 대해 최초 침해 시점 이후의 공격자 행적을 파악하는데 도움이 된다.

6) 불법 사이트 방문 금지

불법 소프트웨어 관련해서 구글 검색을 할 경우 CryptBot 악성코드, BlueCrab 랜섬웨어 등의 유포페이지가 상위에 노출되어 사용자의 접근이 쉽다.

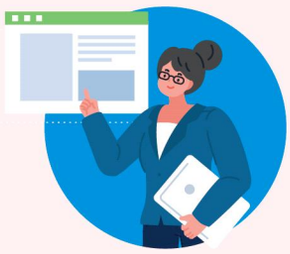
공격자는 취약한 서버나 광고 링크 등을 통해 악성코드를 유포하고 있으며 불법 소프트웨어, 크랙 프로그램 등의 검색어를 통해 사용자를 유인하는 경우가 많고 불법소프트웨어의 보안성을 보장할 수 없으므로 의심스런 사이트에 방문하지 말고 정품 및 검증된 소프트웨어만 사용한다.

7) 감염 후 재발 방지

랜섬웨어에 감염이 되었다면 반드시 감염된 경로를 파악하고 비밀번호를 변경하거나 전체 시스템에 대한 보안성 검토를 진행해야 한다. 감염 경로에 대한 파악 없이 복구만을 했을 때는 같은 방식으로 다시 감염될 수 있다.

5. 정 리

이러한 보안 수칙들은 당연해 보이지만 실 업무환경에 적용하고 지키는 것이 쉽지 않을 수도 있다. 그러나 공격자는 막대한 금전적인 이익을 목적으로 하여 매우 활발하게 새로운 기법과 공격 대상을 찾고 있으며 공격가치가 큰 기업을 상대로 APT 공격을 하는 사례가 많으므로 약간의 방심과 틈 만으로도 큰 피해가 발생할 수 있다는 점에 유의해야 한다.



2022년
사이버보안 대연합

정책제도 분과

1. 일본의 위협정보 공유체계 [최수민 연구원, 인하대학교 디지털혁신전략센터]

일본의 위협정보 공유체계

최수민 연구원, 인하대학교 디지털혁신전략센터, sumin928@gmail.com

1. 법적근거

- 일본은 2000년대 초반 “e-Japan 구상(e-Japan 構想)”[5]을 발표하고, “IT 기본법”을 제정하면서 사이버보안에 적극적으로 대응하기 시작
  - 이전에는 사이버보안에 대한 국가적 차원에서의 대응은 전무
  - “e-Japan 구상”에 기초하여 “고도 정보통신 네트워크 사회 형성 기본법(高度情報通信ネットワーク社會形成基本法, IT 기본법)”을 제정
  - 2005년 4월 NISC(National Information Security Center, 정보보안센터)를 설립하여 사이버보안 정책 추진을 총괄하고, 5월에는 IT 전략본부[6] 내에 “정보보안 정책회의”를 설치하여 국가적 관점에서 사이버보안 기본 전략을 수립[7]

- 2005년 12월, 정보보안 정책회의는 IT 기본법의 정보보안 시책에 따라 “중요 인프라 정보보안과 관련된 행동계획(重要インフラの情報セキュリティ対策に係る行動計画)”을 발표하며 관민이 협력하여 **IT 장애 관련 정보를 공유**할 것을 촉구[8]
  - “IT 장애”를 “주요 인프라의 각 사업에서 발생하는 서비스 정지나 기능 저하 등의 장애 중 IT의 기능 장애를 일으키는 것”이라고 정의하고 이에 대한 정보는 아래의 세 가지를 포함
    ① 미연 방지(未然防止) : 장애 발생 위협에 관한 정보(방호책 등을 포함)
    ② 확대 방지·복구(拡大防止・復旧) : 장애 발생 후의 영향 전파 예측 및 복구에 기여하는 정보
    ③ 재발방지(再発防止) : 사후분석에 필요한 정보의 공동 수집 및 분석·검증 결과
  - 정보공유 체계는 각 주체의 기능을 최대한 활용하면서 각 주체의 역할을 명확히 하고, 특정 주체에 과도한 부담이 발생하지 않도록 정립

5) 일본 정부가 내건 일본형 IT 사회의 실현을 목표로 하는 구상으로 2000년 9월 당시 내각총리대신(모리 키로)이 양원 본회의에서 진행한 소신 표명 연설. 이후 2001년 IT전략본부에서 이를 기반으로 “e-Japan 전략(e-Japan 戦略)”을 발표하며 공식적인 국가전략으로 책정
6) IT 기본법에 의해 설립된 기구로서, 정식명칭은 “고도정보통신네트워크사회 추진전략본부”
7) 정보보안 정책회의와 NISC는 내각관방을 중심으로 한 정부차원의 통합 사이버보안 추진기구. 정보보안 정책회의에서 중장기계획을 수립하고 NISC에서 실무를 담당
8) IT전략본부에서 2005년 9월 발표한 “인프라 정보 보안 대책에 관한 기본적 생각(重要インフラの情報セキュリティ対策に係る基本的考え方)”을 토대로 주요 인프라 사업에서 발생하는 IT 장애가 국민 생활이나 사회 경제 활동에 영향이 미치지 않도록 주요 인프라를 보호하고 주요 인프라 사업자의 지속적인 사업 활동을 위한 대책

① 주요 인프라 사업자에서 소관 부처로의 정보제공은 각 부처별로 선임된 **연락원[9]이 CEPTOAR**를 통해 소관 분야에서 공유

② 조기경계정보 등 **시급한 사안의 경우에는 내각관방에서 직접** CEPTOAR 또는 개별 주요 인프라 사업자에게 제공하며, 정보제공처와 내각관방 간 정보 취급에 관한 규정을 사전 합의

③ 정보 참조자가 해당 정보의 활용이 용이하도록 중요도나 종류, 성격 등에 따라 **정보의 분류 및 취급범위 등 식별방법의 적정화**를 도모

- 이후, 2013년 미국의 행정명령[10]에 자극을 받아 **사이버보안 거버넌스**를 강조한 "사이버보안 전략(サイバーセキュリティ戦略)"을 발표

  - 스마트시티, ITS 등 새로운 정보화 서비스, 방위, 에너지 산업 등 그동안 주요 기반 사업자로 속하지 않았던 분야에 대해 안전기준 책정 및 평가, **정보공유 체제의 심화 및 확충** 등 요구
  - **IT 장애정보 및 공격·위협·취약성 등에 관한 정보**는 주요기반 사업자와 CEPTOAR[11] 간에 지속적으로 정보 공유
  - 업종간 정보공유가 어려운 표적형 공격에 관한 정보는 **비밀유지 계약을 기초로 하는 정보공유 체제**를 심화·확충
  - 주요기반 사업자의 담당 부처에 대한 신속한 보고 및 관계기관과의 정보공유는 **개인정보·비밀정보를 배려**한 후에 촉진
  - 주요 기반 사업자의 CSIRT(Computer Security Incident Response Team, 컴퓨터 보안 사고 대응팀) 간에 사이버 연습을 실시해 사이버 공격에 대한 연계 대응 능력 강화

- 사이버보안 전략은 매년 수정·보완되어 발표되었고, 2015년에는 이를 기반으로 **"사이버보안 기본법(サイバーセキュリティ基本法)"**을 제정

  - "사이버보안"을 "전자적 방식, 자기적 방식, 기타 사람의 지각으로는 인식할 수 없는 방식으로 기록되거나 발신·전달 또는 수신되는 정보의 누설, 멸실 또는 훼손의 방지, 그 밖에 해당 정보의 안전관리를 위하여 필요한 조치와 정보 시스템 및 정보통신 네트워크의 안전성 및 신뢰성 확보를 위하여 필요한 조치가 마련되고 그 상태가 적절히 유지·관리되는 것"으로 정의

  - 사이버보안 시책은 **IT 기본법의 기본 이념을 준수**하고, 국민의 권리를 부당하게 침해하지 않는 수준에서 시행하여 아래의 범위를 포함하여 관련 시책을 강구

9) 리에종(リエゾン)이라고 하며, 내각관방이 겸임

10) 2013년 초 미국의 주요 언론사에 대한 사이버 공격이 이슈가 되며 오바마대통령은 물리적 또는 가상의 국가적 자산을 보호하기 위한 행정명령(행정명령 13636)을 시행하여 정부기관이 사이버위협 관련 정보를 민간과 공유하도록 명령

11) Capability for Engineering of Protection, Technical Operation, Analysis and Response(セプター, 셉터). 주요 인프라 분야에서 사이버보안 관련 정보를 공유하고 분석하는 체제로 ISAC과 유사

① **(국가 행정기관 등에서의 사이버 시큐리티의 확보)** 국가 행정기관, 독립행정법인 및 지정법인의 사이버보안 기준 수립, 국가 행정기관의 정보시스템 공동화(共同化), 정보시스템에 대한 부정한 활동의 감시 및 분석, 사이버보안 훈련 및 국내외 관계기관과 연대, 사이버보안 위협 대응, **국가 행정기관, 독립행정법인 및 지정법인 간 사이버보안에 관한 정보공유**와 그 밖에 필요한 시책

② **(중요 사회 기반 사업자 등의 사이버보안 확보 촉진)** 국가는 중요 사회 기반 사업자 등의 사이버보안 기준 수립, 사이버보안 훈련, 정보공유, 자주적인 대처를 촉진

③ **(민간사업자 및 교육연구기관 등의 자주적인 대처 촉진)** 국가는 민간사업자와 교육연구기관 등에 사이버보안의 중요성에 관한 관심과 이해의 증진, 사이버보안에 관한 상담에 응하며 필요한 정보와 조언을 제공

④ **(다양한 주체의 연대 등)** 국가는 **관계부처 간의 연대를 강화**하고 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련 사업자 등 **다양한 주체가 서로 연대**하여 사이버보안 시책에 대처할 수 있는 방안을 강구

⑤ **(범죄 단속 및 피해 확대 방지)** 국가는 사이버보안에 관한 범죄 단속 및 그 피해 확대 방지를 위하여 필요한 시책을 강구

⑥ **(일본의 안전에 중대한 영향을 미칠 우려가 있는 사상에 대한 대응)** 국가는 일본의 안전에 중대한 영향을 미칠 우려가 있는 사상에 대한 대응을 위해 관계기관 간 연대강화와 역할 분담을 명확화

- 사이버보안 시책을 종합적이고 효과적으로 추진하기 위하여 "사이버보안 전략본부(サイバーセキュリティ戦略本部)[12]"를 설립하고 아래의 업무를 수행

① 사이버보안 전략의 수립 및 추진에 관한 일
② 국가 행정기관, 독립행정법인 및 지정법인의 사이버 보안에 관한 대책마련 및 그에 따른 시책의 평가(감사를 포함), 그 밖에 해당 기준에 따른 시책의 추진에 관한 일
③ 국가 행정기관, 독립행정법인 또는 지정법인에서 발생한 사이버보안 침해사고에 대한 시책의 평가(원인 규명을 위한 조사를 포함)에 관한 일
④ 제1호부터 제3호까지에 해당하는 업무 외에 사이버보안 시책의 조사심의, 부처 통합적인 계획, 관계 행정기관의 경비 견적 방침, 시책 실시에 관한 지침 작성 및 시책의 평가, 그 밖에 해당 시책의 추진 및 종합조정에 관한 일

- 사이버보안 전략 수립 및 추진 내용은 다음의 사항을 포함

① 사이버보안 시책에 대한 기본 방침
② 국가 행정기관 등에서의 사이버보안 확보에 관한 사항
③ 주요 사회 기반 사업자와 그 단체 및 지방공공단체의 사이버보안 확보 촉진에 관한 사항
④ 제1호부터 제3호까지의 사항 외에 사이버보안 시책을 종합적이며 효과적으로 추진하기 위해 필요한 사항

12) 동 법에 따라 기존에 IT기본법에 따라 설치되었던 정보보안 정책회의는 폐기되고 사이버보안 전략본부가 신설되고, NISC는 정보보호센터(National Information Security Center)에서 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity)로 변경

2. 운영기관(공유체계)

2005년 중요 인프라 정보보안과 관련된 행동계획을 통해 CEPTOAR의 역할을 정비하고, CEPTOAR-Council(주요 인프라 연락협의회)를 창설

- **CEPTOAR**는 정부가 제공하는 사이버보안 **정보를 주요 인프라 사업자에게 전달**하고, 관련 주요 인프라 사업자의 서비스 유지 및 복구 능력 향상에 이바지하기 위한 목적으로 설치

① 내각관방이 제공하는 정보의 취급에 관한 결정, 기밀유지 및 외부로의 정보제공에 관해 구성원 간에 합의된 규칙이 존재

② 긴급 시에 각 구성원 및 외부와의 연락이 가능한 창구(POC, Point of Contact)를 사전에 설정

[표 1] CEPTOAR의 주요 역할과 내용

1. '장애 대응 체제의 강화'에 관한 사항

① 임무보증을 위한 '면으로서의 방호'를 염두에 두고 서플라이 체인을 포함한 방호범위 재검토 노력에 대한 적극적인 협력.

2. '정보공유체제 강화'에 관한 사항

① CEPTOAR-Council, 주요 인프라 사업자 등 주요 인프라 소관 부처 및 내각관방과 연계하여 평상시 및 대규모 주요 인프라 서비스 장애 대응 시의 정보공유 체제 운용.

② 내각관방 등으로부터의 정보 제공에 대해 CEPTOAR 내의 정보 취급 규칙에 따라 주요 인프라 사업자 등에 대한 정보 제공 실시.

③ 주요 인프라 사업자 등으로부터의 정보 연락에 대해 필요에 따라 CEPTOAR 사무국에서 익명화 등을 실시한 후 주요 인프라 소관 부처에 보고하고 CEPTOAR 구성원에 대한 전개 등 정보공유 체제를 강화.

④ 사이버보안 관계기관과의 합의에 기초한 보완적인 정보공유 실시.

⑤ CEPTOAR의 기능 강화 및 충실.

⑥ 내각관방이 실시하는 각 CEPTOAR의 기능이나 활동 상황을 파악하기 위한 조사·청취 등에 대한 협력.

⑦ CEPTOAR-Council 참가.

⑧ 정보 소통 기능의 정기적인 확인.

3. '리스크 관리의 활용'에 관한 사항

① 자체 CEPTOAR를 구성하는 주요 인프라 사업자 등의 주체적인 대응을 지원. 또한 필요에 따라 내각관방, 주요 인프라 소관 부처, 다른 CEPTOAR, 기타 관계 주체에 대한 협력.

4. '방호 기반 강화'에 관한 사항

① 주요 인프라 사업자 등의 분야 횡단적 연습 참가를 지원.

② 필요에 따라 분야 횡단적 연습 참가.

③ 분야 횡단적 연습에서 얻은 주요 인프라 보호에 관한 지식의 보급·전개를 지원.

- CEPTOAR-Council을 창설하여 각 주요 인프라 분야별 서비스의 유지·복구 관련 정보 중 복수의 **주요 인프라 분야에 공통되는 정보공유**를 실시

[표 2] CEPTOAR-Council의 주요 역할과 내용

1. '정보공유체제 강화'에 관한 사항

① 각 CEPTOAR와 연계하여 평상시 및 대규모 주요 인프라 서비스 장애 대응 시의 정보공유 체제 운용.
② 공유 대상으로 하는 정보 및 그 공유 방법의 정리 실시.
③ 상호 이해 및 베스트 프랙티스 등의 구체적인 사례 공유를 통한 분야 횡단적인 정보 공유 추진.
④ 관계 주체와의 협력관계를 돈독히 하기 위해 정부기관 등의 요청 또는 스스로의 발의에 의해 양자의 상황인식 등의 공유를 추진하기 위한 의견교환 등의 실시.

2. '방호 기반 강화'에 관한 사항

① 필요에 따라 분야 횡단적 연습 참가

중요 인프라 정보보안과 관련된 행동계획은 이후 지속적으로 개정[13]되어 "중요 인프라의 정보보안 대책에 관한 제4차 행동계획"까지 발표되었으며, 2022년 6월에는 기존의 행동계획을 보완하여 "중요 인프라 사이버 보안과 관련된 행동 계획(重要インフラのサイバーセキュリティに係る行動計画)"을 발표

- 공유해야 할 정보를 "중요 인프라 서비스 장애를 포함한 시스템의 오류나 전조 등에 관한 정보"라고 정의
- "주요 인프라"를 14개 분야로 규정하고, 이를 보호하기 위한 대응 방안을 제시

[표 3] 주요 인프라별 소관부처

소관부처	분 야
내각부	금융
경제산업성	전력, 가스, 수도, 화학, 신용, 석유
총무성	정부·행정 서비스, 정보통신
후생노동성	의료
국토교통청	철도, 항공, 물류, 공항

13) 2015년에는 IT기본법에서 사이버보안기본법으로 소관 법령이 이관

[표 4] 주요 인프라 소관부처의 대처사항

1. '장애 대응 체제의 강화'에 관한 사항

① 주요 인프라 사업자 등의 BCP/IT-BCP, CSIRT, 감사체제 등의 정비에 관한 대응 지원.
② 위협의 검지·조사·분석에 관한 능력의 향상.
③ 방어력, 억제력, 상황 파악력 향상.
④ 임무보증을 위한 '면으로서의 방호'를 확보하기 위한 대응 계속.
⑤ 주요 인프라 분야 내에서 실제로 대처하는 대상인 '주요 인프라 사업자 등'의 범위에 대해 지속적으로 재검토.

2. '안전기준 등의 정비 및 침투'에 관한 사항

① 안전기준 등 책정지침으로서 새롭게 자리매김할 수 있는 안전기준 등에 관한 정보 등을 내각관방에 제공.
② 스스로가 안전기준 등의 책정주체인 경우에는 정기적으로 안전기준 등의 분석·검증을 실시하는 것과 더불어 필요에 따라 안전기준 등의 개정을 실시.
③ 주요 인프라 분야별 안전기준 등의 분석·검증 지원.
④ 주요 인프라 사업자 등에 대해 대책을 실장하기 위한 환경정비를 포함한 안전기준 등의 침투를 위한 대응.
⑤ 매년 내각관방이 실시하는 안전기준 등의 계속적 개선 상황 파악에 협력.
⑥ 매년 내각관방이 실시하는 주요 인프라 사업자 등의 안전기준 정비상황 및 사이버보안 확보를 위한 대응과 수단에 대한 조사방법 검토 및 실시에 협력.

3. '정보공유체제 강화'에 관한 사항

① 내각관방과 연계하여 평상시 및 대규모 주요 인프라 서비스 장애 대응 시의 정보공유 체제 운용.
② 주요 인프라 사업자 등과의 긴밀한 정보 공유 체제 유지와 필요에 따른 재검토.
③ 주요 인프라 사업자 등으로부터의 시스템 오류 등에 관한 정보를 내각관방에 확실한 연락.
④ 내각관방이 실시하는 각 CEPTOAR의 기능이나 활동 상황을 파악하기 위한 조사·청취 등에 대한 협력.
⑤ CEPTOAR의 기능 충실에 대한 지원.
⑥ CEPTOAR-Council 지원.
⑦ CEPTOAR-Council 등의 요청이 있을 경우 의견교환 등을 실시.
⑧ CEPTOAR 사무국이나 주요 인프라 사업자 등의 정보공유에 관한 활동에 대한 협력.
⑨ 내각관방이 정보 소통 기능 확인(셉터 훈련) 등의 기회를 제공하는 경우의 협력.

4. '리스크 관리의 활용'에 관한 사항

① 리스크 평가를 실시할 때 내각관방, 주요 인프라 사업자 등 기타 관계 주체가 실시하는 대응에 대한 협력.
② 내각관방에 의해 제공된 가이던스 등 주요 인프라 사업자 등에 대한 전개 및 기타 리스크 평가의 침투에 기여하는 내각관방에 대한 필요한 협력.
③ 주요 인프라 사업자 등의 리스크 커뮤니케이션 지원.
④ 주요 인프라 사업자 등이 실시하는 모니터링 및 리뷰 필요에 따른 지원.
⑤ 본 시책의 조사 등에 관해 해당 조사 등에 관한 정보 및 필요한 정보를 내각관방에 제공하는 등의 협력. 또한 주요 인프라 소관 부처가 실시하는 조사·분석이 본 시책의 조사 등과 관련된 경우에는 필요에 따라 내각관방과 연계.
⑥ 본 시책의 조사 등을 시책에 활용.

5. '방호 기반 강화'에 관한 사항

① 분야 횡단적 연습의 시나리오, 실시 방법, 검증 과제 등의 기획, 분야 횡단적 연습의 실시에 대한 협력.
② CEPTOAR 및 주요 인프라 사업자 등의 분야 횡단적 연습 참가를 지원.
③ 분야 횡단적 연습 참가.
④ 필요에 따라 분야 횡단적 연습 성과를 시책에 활용.
⑤ 분야 횡단적 연습 개선책 검토에 대한 협력.
⑥ 분야 횡단적 연습과 주요 인프라 소관 부처가 실시하는 주요 인프라 보호에 이바지하는 연습·훈련과의 상호 연계에 대한 협력.
⑦ 사이버 보안과 관련된 연습이나 교육 등을 통해 사이버 보안 인재의 육성을 지원.
⑧ 주요 인프라 사업자 등에 대한 '보안 바이 디자인'의 구현 추진.
⑨ 내각관방과 연계해 각국 정부 등과의 협력·연계를 강화하고, 지식 공유 및 능력 구축 지원 등을 추진.
⑩ 내각관방과 연계하여 관련 규격의 정리, 가시화.

- 2018년 12월 사이버보안기본법 일부를 개정하여 사이버보안협의회(サイバーセキュリティ協議会) 설립 및 사이버보안 정보공유 활성화를 위한 법적 환경을 마련[14)]

- **국가 행정기관, 중요 사회 기반사업자, 사이버관련 사업자 등 관련 주체가 상호 연계하여 신속하게 사이버보안 관련 정보를 공유**하여 사이버 공격에 의한 피해를 예방하고 피해 확대를 막는 목적
- 협의회에서는 2022년 현재 303개 기업이 가입되어 있다고 밝혔으며, 구체적인 **명부는 비공개**[15)]
- 협의회 사무국은 JPCERT/CC에서 담당하며, 3개 레벨로 구분된 구성원과 운영위원회 등으로 구성

[표 5] 사이버보안협의회 구성

구 분		역 할
사무국(JPCERT/CC)		관련 업무를 총괄
운영위원회		구성원 가입 승인 또는 철회, 정보제공 등 협력 요청
Task Force 구성		제1구성원 + 제2구성원 (해외자본출자 법인은 참여 불가가 원칙이나, 장기간 고도의 신뢰관계 구축 & 특별 승인을 획득한 자 제외)
구성원	제1구성원 (NISC, JPCERT/CC포함)	아직 검증되지 않은 전문적인 분석내용 등을 제공하고 구체적 대응방안 작성 (내부적으로 수집/분석한 시나리오 정보 등)
	제2구성원	제1구성원으로부터 공유받은 대응방안 정보에 대한 피드백, 해당 정보를 활용하여 초기 대응
	일반 구성원	평시에 관련 정보를 수령하여 자체적으로 대책 마련 (대규모 사이버공격 발생 시 정보제공)

14) https://www.nisc.go.jp/council/cs/kyogikai/index.html
15) 협의회 명부는 협의회 시스템에 게재하고 협의회 구성원만 열람할 수 있으나 협의회 구성원이 자신이 협의회의 구성원이라고 공표하는 것은 무방

사이버보안협의회에서는 민간기업 간 사이버보안 정보공유를 위한 구체적인 절차와 방법을 제시

- 시스템의 오류 등에 관한 정보 중 이하의 어느 하나에 해당하는 경우, 주요 인프라 사업자 등은 **정보 연락을 실시**[16)]

① 법령 등에서 주요 인프라 소관 부처에 의무적으로 보고해야 할 경우

② 관계 주체가 국민생활이나 주요 인프라 서비스에 심각한 영향이 있다고 판단하거나, 주요 인프라 사업자 등이 정보를 공유하는 것이 적절하다고 판단했을 경우

③ 그 외 주요 인프라 사업자 등이 정보를 공유하는 것이 적절하다고 판단했을 경우

- 주요 인프라 사업자 등으로부터 주요 인프라 소관 부처를 통해 내각관방에 이르는 **정보 연락 절차**는 다음의 순서

① 주요 인프라 사업자는 아래의 정보연락을 위한 침해사고 유형과 원인 유형에 따라 해당 원인을 유형화한 후 소관 부처에 연락

[표 6] 정보연락을 위한 침해사고 유형

구 분		사고 예	설 명
침해사고 미발생		전조	사이버 공격 예고 등 전조나 침해사고에는 이르지 못한 실수, 악성 메일이 첨부된 의심 메일 수신 등
침해 사고 발생	기밀성을 위협하는 사고	정보의 누설	조직의 기밀정보 등의 유출 등 기밀성이 위협받는 사고의 발생
	완전성을 위협하는 사고	정보의 파괴	Web 사이트 등의 조작이나 조직의 기밀정보 파괴 등 완전성을 위협받는 사고의 발생
	가용성을 위협하는 사고	시스템 이용 곤란	제어 시스템이 가동 불가능하거나 Web 사이트의 열람이 불가능한 등 가용성이 위협받는 사고 발생
	위에 이어지는 사고	악성코드 감염	악성코드 등에 의한 시스템 감염
		부정코드 실행	시스템 취약성 등을 지적한 악성코드 실행
		시스템 침입	외부의 사이버 공격 등에 의한 시스템 침입
		기 타	그 외의 침해사고

16) 정보연락은 그 시점에서 판명된 사상이나 원인을 기준으로 수시로 연락하며, 전체 내용이 판명되기 전의 단편적이거나 불확실한 것이어도 무방

[표 7] 침해사고 원인 유형

원인유형	예 시
의도적인 원인	의심 메일 등의 수신, 사용자 ID 등의 거짓, DDoS 공격 등의 대량 액세스, 정보의 부정 취득, 내부 부정, 적절한 시스템 등 운용의 미실시 등
우발적인 원인	사용자의 조작 실수, 사용자의 관리 실수, 의심스러운 파일의 실행, 의심스러운 사이트의 열람, 외부 위탁처의 관리 실수, 기기 등의 고장, 시스템의 취약성, 타 분야의 장애로부터의 파급 등
환경적인 원인	재해나 질병 등
기타 원인	상기 이외의 위협이나 취약성, 원인 불명 등

② 소관 부처에서는 분야별로 선임된 연락원을 통해 사업자로부터 받은 정보를 내각관방에 연락

③ 내각관방은 연락된 정보를 적절히 관리하고 규정에 따라 정보공유가 가능한 범위에서 취급

④ 긴급성이 있는 경우에는 ①~②의 절차에 관계없이 주요 인프라 사업자가 소관 부처에 연락하고 내각관방에도 직접 통보

- 내각관방에서 받은 정보를 주요 인프라 사업자에 전달하는 정보제공 절차는 다음의 순서

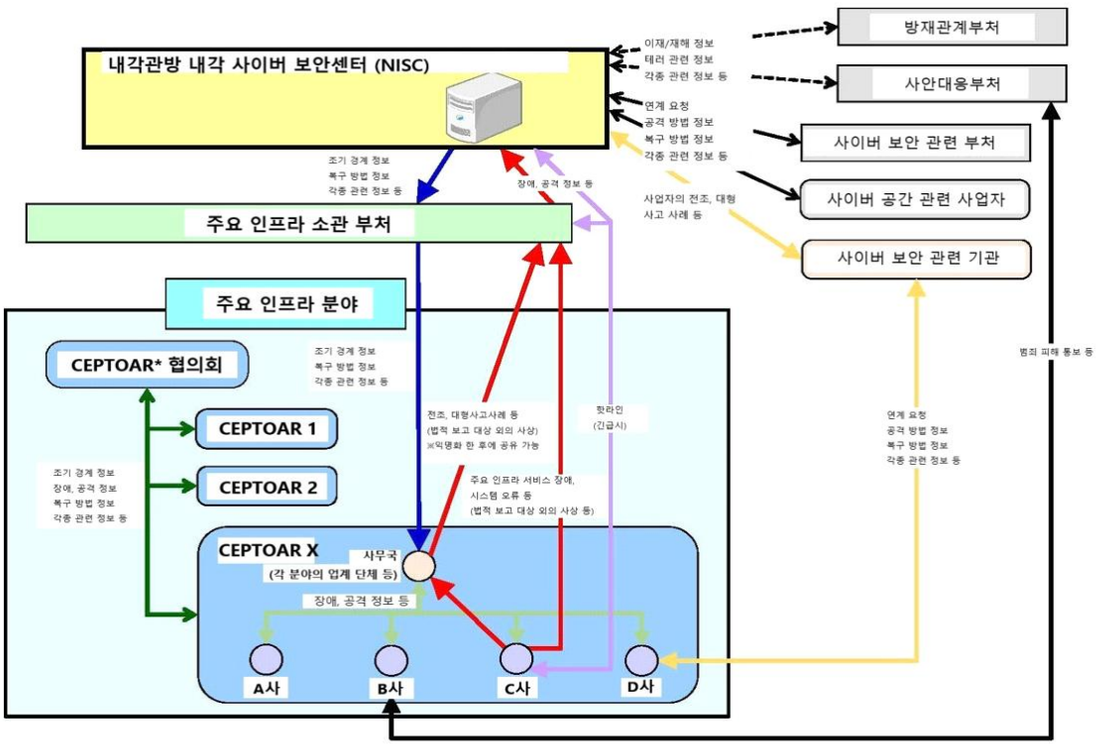
① 정보의 제공은 주요 인프라 소관 부처의 연락원을 통해 실시

② 연락원은 CEPTOAR PoC에 정보를 전달

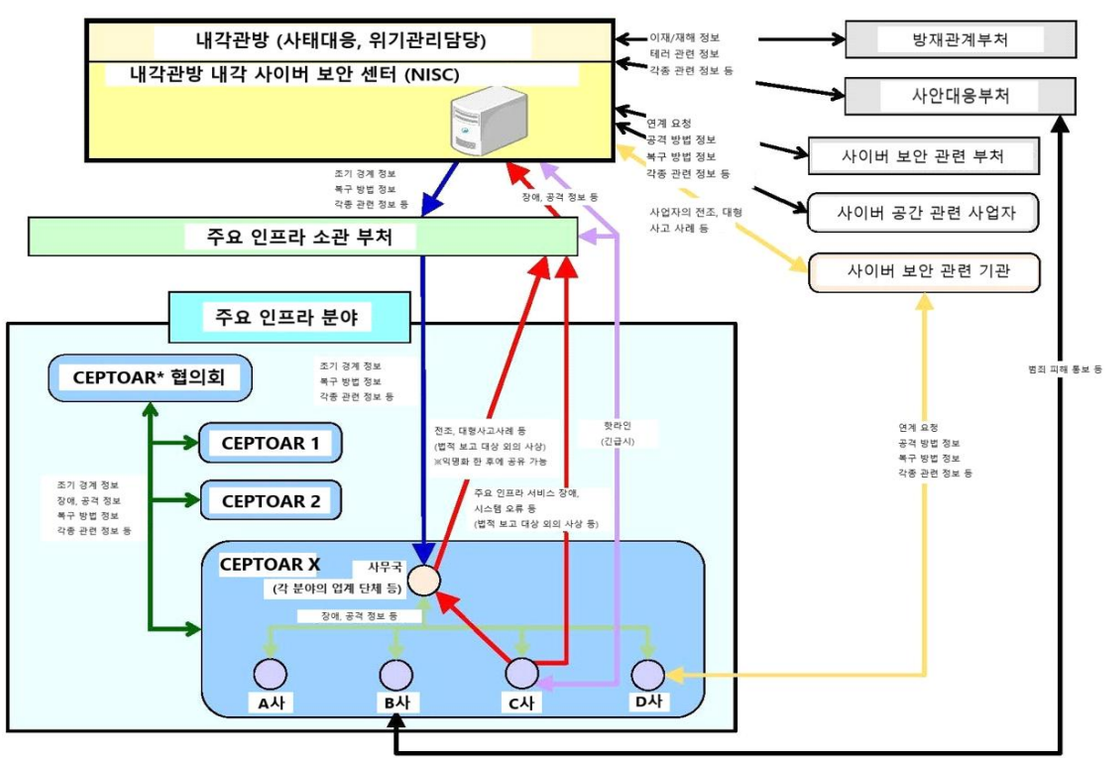
③ CEPTOAR는 CEPTOAR를 구성하는 주요 인프라 사업자에게 정보를 전달

④ 긴급성이 있는 조기경계정보는 ①~③의 절차에 관계없이 내각관방에서 직접 CEPTOAR 또는 개별 주요 인프라 사업자에게 제공

[그림 1] 정보공유절차(평상시)



[그림 2] 정보공유절차(사고 발생 시)



[표 8] 관계 주체별 역할

관계 주체	평시의 역할	침해사고 대응 시 역할
내각 관방 (사태 대처· 위기관리 담당)	주요 인프라와 관련된 사안 정보에 대해 NISC와 상호 정보를 공유	평상시의 역할과 더불어 NISC와 일체화하여 사안대처부처 및 방재관계부처로부터 제공되는 피해정보, 대응상황정보 등을 집약하여 NISC와 상호 정보를 공유
내각 관방 (NISC)	주요 인프라 관할부처, 정보보안 관계부처, 사안대처부처, 방재관계부처, 정보보안 관계기관 및 사이버공간 관련 사업자 등과 상호 시스템 오류 등에 관한 정보를 공유	내각관방과 일체화하여 주요 인프라 소관부처, 정보보안 관계부처, 사안대처부처, 방재관계부처, 정보보안 관계기관 및 사이버공간 관련 사업자 등과 상호 시스템의 오류 등에 관한 정보를 공유
주요 인프라 관할 부처	소관하는 주요 인프라 사업자 등으로부터 수령한 정보를 NISC 및 해당 CEPTOAR에 연락하고, NISC로부터 수령한 정보를 해당하는 CEPTOAR에 제공	평시의 역할과 더불어 필요에 따라 대규모 주요 인프라 서비스 장애 대응 시의 체제에 협력
CEPTOAR- Council[17]	CEPTOAR-Council의 주체적인 판단에 따라 각 CEPTOAR가 적극적으로 참여하여 주요 인프라 사업자 등에서의 서비스 유지·복구를 위한 폭넓은 정보를 공유	평상시의 역할과 더불어 필요에 따라 대규모 주요 인프라 서비스 장애 대응을 위한 체제를 구축하고, CEPTOAR를 비롯한 관계기관과의 연계를 도모
CEPTOAR 사무국	주요 인프라 관할 부처, 사안 대처 부처, 방재 관계 부처, 정보 보호 관계 기관, CEPTOAR Council 및 주요 인프라 사업자와 연계하여 정보 공유	평상시의 역할과 더불어 필요에 따라 대규모 주요 인프라 서비스 장애 대응을 위한 체제를 구축하고 관계기관과 연계를 도모
주요 인프라 사업자 등	필요에 따라 소속된 CEPTOAR 내에 공유하고, 주요 인프라 소관 부처에 연락하고, 범죄 피해를 당했을 경우에는 사안 대처 부처에 통보	평상시의 역할과 더불어 필요에 따라 대규모 주요 인프라 서비스 장애 대응을 위한 체제를 구축하고 관계기관과 연계를 도모

17) CEPTOAR-Council은 정부기관을 포함해 다른 기관의 하위에 위치하는 것이 아니라 독립된 회의체이며, 각 CEPTOAR의 주체적인 판단에 따라 연계

3. 재원조달

- 사이버보안기본법 제12조 6항에서 정부는 사이버 시큐리티 전략에 대하여 실시에 필요한 경비에 관하여 필요한 자금을 확보하기 위하여 매년도 국가 재정이 허락하는 범위 내에서 이를 예산에 계산하는 등 원활한 실시에 필요한 조치를 강구, 노력하도록 명기[18)]

- 사이버보안협의회 가입 등 관련 기관에 등록하여 **정보공유를 받는 과정은 무료**로 진행

- 다만, 침해사고로 인한 네트워크 차단, 증거 보전, 피해 확대 방지 등 초동 대응에 필요한 대응은 일본 정부[19)]가 지정한 사고리스폰스사업자(インシデントレスポンス事業者)에게 지원받을 수 있으며, 사고리스폰스사업자에게 비용을 지급[20)]

4. 공유정책(공유정보)

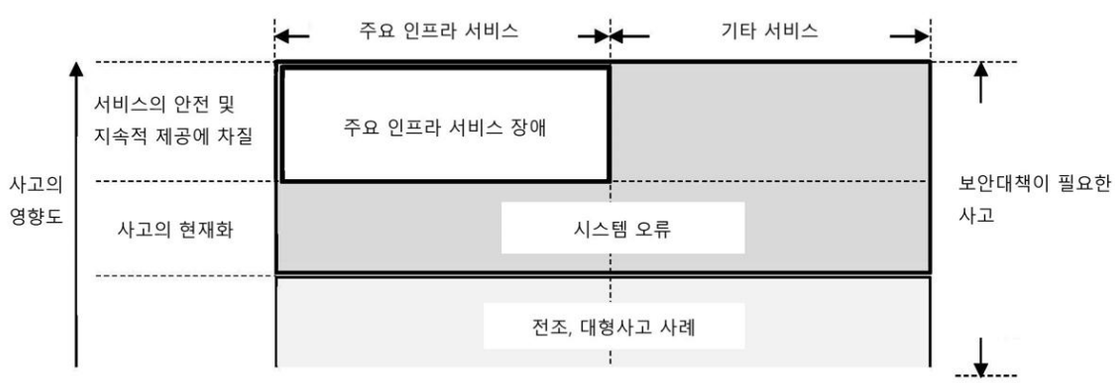
- 내각관방 및 정보를 공유받은 주요 인프라 소관 부처는 법령에 규정이 있거나 정보제공원의 승낙이 있는 경우를 제외하고 정보 내용은 비공개로 하는 것이 원칙
  - 해당 정보는 「행정기관이 보유한 정보의 공개에 관한 법률」에 따른 비공개정보로 구분
  - 다만, 해당 정보가 같은 호 단서에서 규정하는 정보 12에 해당하거나 아래의 정보 제공을 실시하는 경우 등에 해당하면 예외
    ① 보안 취약점이나 프로그램 버그 등에 관한 정보를 입수하고, 다른 주요 인프라 사업자도 관련된 중대한 문제가 발생할 우려가 있다고 인정되는 경우
    ② 사이버 공격의 발생 또는 공격의 예고가 있는 경우, 재해에 의한 피해가 예측되는 경우 등 다른 주요 인프라 사업자의 중요 시스템이 위험에 노출되어 있다고 인정되는 경우
    ③ 그 밖에 주요 인프라 사업자의 사이버 보안 확보에 효과적이라고 생각되는 경우

18) 세부적인 예산은 비공개
19) 일본 JNSA(일본 네트워크 보안협회, Japan Network Security Association)와 IPA(정보처리추진기구, Information-technology Promotion Agency)는 정보보안 서비스 기준에 적합한 것으로 인정된 사고리스폰스사업자 목록을 제공
20) https://www.jnsa.org/emergency_response/

- 내각관방 및 정보의 제공원이 특정되지 않도록 정보를 가공하는 등 불이익을 받지 않기 위한 적절한 조치를 강구한 후 정보를 제공
  - 정보제공 범위는 정보제공원이 미리 제시하는 정보공유 가능한 범위 중 내각관방이 해당 정보와 관련있는 주요 인프라 분야
  - 정보제공원이 제시하는 정보공유 가능한 범위를 넘어 정보를 공유할 필요가 있다고 내각관방이 인정하는 경우에는 정보제공원과 조정

- 사이버보안협의회에 참여한 사업자가 **안심하고 정보를 제공**할 수 있도록 정보제공원이 정보제공 범위를 설정할 수 있도록 하고, 정보제공 의무가 적용되는 경우 등 법적 의무사항을 규정에서 명확하게 제시
  - 정보를 공유하는 구성원은 사이버보안기본법 벌칙규정에 근거하여 **기밀유지 의무**사항 준수 의무[21)]
  - 설정된 정보의 **공유범위는 무단 변경 금지**
  - 정보를 제공한 사업자는 사이버보안협의회를 통해 대응방안에 대한 조언 및 현황에 대한 피드백을 획득
  - 정보제공의무가 적용되는 경우는 “대규모 사이버공격”, “정보제공원이 동의한 경우” 등으로 한정

[그림 3] 행동계획에 따른 정보공유의 범위



21) 이를 위반하는 경우, 1년 이하의 징역 또는 50만엔 이하의 과태료

또한 주요 인프라 서비스 장애의 심각도나 해당 장애에 관한 정보의 중요도에 따라 영향 범위나 대처 행동 등이 달라진다는 점을 감안하여 아래와 같이 주요 인프라 서비스 장애와 관련된 심각도 판단기준의 예를 마련

[표 9] 주요 인프라 서비스 장애에 관한 심각도 판단 기준

구 분	기 준
레벨1 (저)	주요 인프라 서비스에 영향을 줄 **우려가 작은** 현상
레벨2 (중)	주요 인프라 서비스에 영향을 미칠 **우려가 있는** 현상
레벨3 (고)	주요 인프라 서비스에 **일정한 영향**을 미칠 우려가 높은 현상
레벨4 (중대)	주요 인프라 서비스에 **현저한 영향**을 미칠 우려가 높은 현상
레벨5 (위기)	**여러** 주요 인프라 서비스에 현저한 영향을 미칠 **우려가 절박(切迫)한** 현상

"조기경계정보(早期警戒情報)"는 취약성 정보 혹은 국내외의 보안 기관과의 정보 연계 및 독자적인 트래픽 모니터링 등으로 얻은 위협 정보나 그 대책 등을 중요 인프라 사업자 등을 대상으로 JPCERT 코디네이션 센터(JPCERT/CC)가 제공하는 정보 서비스[22)]

- 조기경계정보의 제공처는 국민의 사회활동에 주요 인프라 사업자의 정보보안관련부서 또는 조직 내 CSIRT이며, 구체적인 제공처는 비공개
- 조기 경계 정보는 각 조직 내의 정보 보안을 추진하는 목적으로 활용하며, CEPTOAR는 CEPTOAR 산하의 주요 인프라 사업자에게의 정보 제공에 활용

[표 10] 조기 경보 정보 제공 대상 조직

- 정부계 조직
- 각종 공공단체(지방공공단체, 공공조합, 영조물법인, 독립행정법인 등)
- CEPTOAR (중요 인프라 14개 분야의 사업자별 정보 공유 및 분석 체제)
- 중요 인프라 사업자
- 중요 인프라와 관련된 제품 개발을 수행하는 사업자
- 중요 인프라 사업자의 대규모 시스템을 구축, 운영하는 사업자
- 산업기기의 제어 등을 실시하는 임베디드 기기의 개발·제공을 실시하고 있는 사업자
- 널리 국민 사회 활동에 관련된 서비스와 인프라를 제공하는 사업자
- 널리 국민에게 이용되는 전자제품이나 제어기기 등을 제공하는 사업자

22) https://www.jpcert.or.jp/wwinfo/

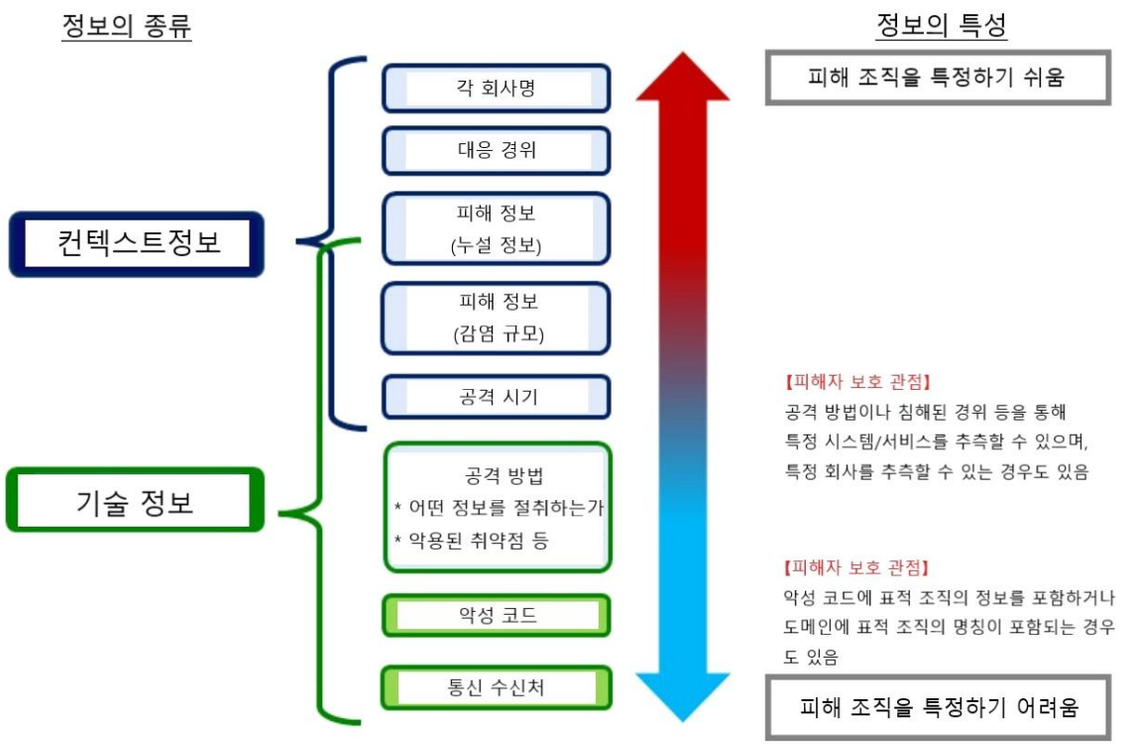
5. 공유방식(표현규격)

- 사이버보안협의회에서 운영하는 중요한 위협 정보를 수집할 수 있는 사용자 한정 포털 사이트(CISTA, Collective Intelligence Station for Trusted Advocates)를 운영[23)]
  - CISTA는 협의회 가입자에 한해 접속 가능하며, 구체적인 공유방식이나 표현 규격 등은 비공개

- 2022년 4월 사이버 공격 피해에 관한 정보의 공유·공표 지침을 마련하기 위해, 사이버보안협의회를 통해 "사이버 공격에 관한 정보의 공유·공표 가이던스(guidance) 검토회(サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会)"를 개최[24)]
  - 사이버 침해사고를 당한 기업은 사고의 피해자이면서, 일반 소비자에게는 가해자가 될 수 있는 어려운 상황이므로 관련 정보를 공유하고 공표하기 위한 지침이 필요하다고 설명
  - 피해 정보(被害情報)를 공격에 사용된 악성코드나 부정통신처 등의 "기술정보(技術情報)"와 피해내용이나 피해조직이 어떠한 대처를 했는지 등의 "컨텍스트 정보(コンテクスト情報)"로 구분
  - 기술정보는 공격 방법을 나타내는 정보를 의미하며, 멀웨어나 부정 통신원 등 새로운 공격 수법의 분석과 대응 방안의 검토 등을 위해 필요
  - 컨텍스트 정보는 피해를 나타내는 정보이며, 피해 조직이 공표하거나 공표 전에 미디어로 보도되는 등 피해 조직의 공표 전에 확산되어 버리는 경우도 존재
  - 공격 수법을 모두 분석하고 침해사고 피해 조직이 2차 피해를 받지 않는 시점이 되면 관련 기술정보는 이미 활용하기 어려울 수 있으므로 새로운 사이버 공격의 수법 등에 관한 기술 정보는 피해 공표보다 더 빠른 단계에서 공유할 필요
  - 따라서 사이버 공격에 관한 정보의 공유·공표 가이던스는 기술정보와 컨텍스트 정보를 구분하여 피해조직의 특정에 연결되지 않는 정보는 조기에 공유한다는 것을 목표로 하는 접근법

23) https://www.jpcert.or.jp/about/06_2.html
24) https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

[그림 4] 기술정보와 컨텍스트 정보



2022년

사이버보안 대연합(2차)

탐지공유 분과
대응역량 분과
정책제도 분과

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회